BỘ THÔNG TIN VÀ TRUYỀN THÔNG

TÀI LIỆU HƯỚNG DẪN
BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG CHO CÁC HỆ THỐNG THÔNG TIN THUỘC PHẠM VI QUẢN LÝ CẤP BỘ, TỈNH

(*Kèm theo Công văn số /BTTTT-CATTT ngày tháng năm 2024 của Bộ Thông tin và Truyền thông)*

Hà Nội, 2024

MỤC LỤC

THUẬT NGỮ, TỪ VIẾT TẮT

STT	Từ viết tắt	Nghĩa đầy đủ
1	Nghị định 85/2016/NĐ-CP	Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ
2	Thông tư 12/2022/TT-BTTTT	Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ
3	TCVN 11930:2017	Tiêu chuẩn quốc gia TCVN 11930:2017 về Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ
4	CNTT	Công nghệ thông tin
5	WAN	Mạng tin học diện rộng
6	LAN	Mạng nội bộ
7	HSĐXCĐ	Hồ sơ đề xuất cấp độ

TÀI LIỆU HƯỚNG DẪN
BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG CHO CÁC HỆ THỐNG THÔNG TIN THUỘC PHẠM VI QUẢN LÝ CẤP BỘ, TỈNH

I. HƯỚNG DẪN CHUNG

1.1. Phạm vi điều chỉnh

Tài liệu này hướng dẫn việc thực thi tổng thể, đồng bộ các biện pháp bảo đảm an toàn thông tin cho các hệ thống thông tin thuộc phạm vi quản lý cấp bộ, tỉnh. Nội dung được hướng dẫn trong tài liệu này bao gồm các nội dung chính sau:

(1) Xác định các hệ thống thông tin thuộc phạm vi quản lý cấp bộ, tỉnh;

(2) Triển khai các biện pháp bảo vệ theo phương án được phê duyệt trong Hồ sơ đề xuất cấp độ;

(3) Tổ chức bảo đảm an toàn thông tin mạng theo mô hình 4 lớp;

(4) Sử dụng các nền tảng quốc gia hỗ trợ bảo đảm an toàn thông tin mạng.

(5) Cơ quan, tổ chức có thể triển khai một số giải pháp tăng cường bảo đảm an toàn hệ thống thông tin được hướng dẫn tại Công văn số 2516/BTTTT-CATTT ngày 27/6/2024 và Công văn số 2517/BTTTT-CATTT ngày 27/6/2024 của Bộ Thông tin và Truyền thông về việc hướng dẫn một số giải pháp tăng cường bảo đảm an toàn hệ thống thông tin.

Các nội dung khác liên quan đến xác định và xây dựng HSĐXCĐ, cơ quan, tổ chức có thể tham khảo tại Công văn số 478/CATTT-ATHTTT ngày 30/3/2024 của Cục An toàn thông tin - Bộ Thông tin và Truyền thông về việc ban hành Sổ tay Hướng dẫn tuân thủ quy định pháp luật và tăng cường bảo đảm an toàn hệ thống thông tin theo cấp độ (Phiên bản 1.0).

1.2. Đối tượng áp dụng

Tài liệu này được xây dựng để hướng dẫn và khuyến nghị áp dụng đối với cơ quan, tổ chức là chủ quản hệ thống thông tin, đơn vị chuyên trách về an toàn thông tin và đơn vị vận hành hệ thống thông tin thuộc phạm vi quản lý cấp bộ, tỉnh.

Cơ quan, tổ chức khác có thể tham khảo tài liệu hướng dẫn này để bảo đảm an toàn hệ thống thông tin tổng thể, đồng bộ, hiệu quả.

1.3. Giải thích từ ngữ

1. Giám sát lớp mạng: Là hoạt động giám sát nhằm thu thập, phân tích và xử lý các gói tin trên đường truyền mạng để phát hiện tấn công mạng, hành vi mã độc trên môi trường mạng; các hình thức tấn công khai thác lỗ hổng phần mềm, dịch vụ trong dữ liệu truyền tải trên mạng thông qua phân tích các dấu hiệu đặc trưng.

Ví dụ một số giải pháp sử dụng trong giám sát lớp mạng có một hoặc một vài chức năng: trích rút dữ liệu; phát hiện xâm nhập; phòng, chống mã độc trên môi trường mạng; quản lý truy cập lớp mạng…

2. Giám sát lớp máy chủ: Là hoạt động giám sát nhằm thu thập, phân tích và xử lý nhật ký hệ thống của máy chủ, hệ điều hành để phát hiện các hoạt động không bình thường, tấn công mạng và các hành vi truy cập trái phép vào máy chủ, hệ điều hành.

Ví dụ một số giải pháp sử dụng trong giám sát lớp máy chủ có một hoặc một vài chức năng: thu thập, phân tích nhật ký hệ thống; phát hiện xâm nhập; phòng, chống mã độc; phát hiện các hành vi bất thường; phát hiện truy cập trái phép vào máy chủ, hệ điều hành…

3. Giám sát lớp ứng dụng: Là hoạt động giám sát nhằm thu thập, phân tích và xử lý nhật ký của máy chủ ứng dụng để phát hiện các truy cập trái phép, tấn công mạng (Tấn công vào lớp ứng dụng như SQLi, XSS...; Tấn công dò quét, vét cạn mật khẩu, thư mục và khai thác thông tin; Tấn công thay đổi giao diện; Tấn công Phishing và cài cắm mã độc trên ứng dụng) và các hành vi bất thường gây nên hoạt động không bình thường của ứng dụng.

Ví dụ một số giải pháp sử dụng trong giám sát lớp ứng dụng có một hoặc một vài chức năng: tường lửa ứng dụng web, tường lửa cơ sở dữ liệu, giải pháp bảo đảm an toàn thông tin cho thư điện tử...

4. Giám sát lớp thiết bị đầu cuối: Là hoạt động giám sát nhằm thu thập, phân tích và xử lý nhật ký hệ thống của thiết bị đầu cuối để phát hiện các truy cập trái phép, tấn công mạng và các hành vi bất thường gây nên hoạt động không bình thường của thiết bị.

Ví dụ một số giải pháp sử dụng trong giám sát thiết bị đầu cuối có một hoặc một vài chức năng: phòng, chống mã độc; phòng, chống xâm nhập; kiểm soát truy cập…

II. CÁC HỆ THỐNG THÔNG TIN THUỘC PHẠM VI QUẢN LÝ CẤP BỘ, TỈNH

Để có thể bảo vệ tổng thể, đồng bộ và đầy đủ các hệ thống thông tin thuộc phạm vi quản lý theo trách nhiệm của chủ quản hệ thống thông tin tại Điều 20 Nghị định 85/2016/NĐ-CP ngày 01/7/2016, cơ quan, tổ chức cần xác định đầy đủ các hệ thống thông tin thuộc phạm vi quản lý.

Để xác định các hệ thống thông tin cần được bảo vệ thuộc trách nhiệm của chủ quản hệ thống thông tin theo quy định, các hệ thống thông tin có thể được chia thành các nhóm hệ thống thuộc phạm vi quản lý cấp bộ, tỉnh, như sau:

- Hệ thống thông tin thuộc phạm vi quản lý của bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ gồm các hệ thống thông tin dùng chung, hệ thống thông

tin phục vụ hoạt động nghiệp vụ và các hệ thống thông tin khác do các đơn vị thuộc phạm vi quản lý của bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ làm chủ đầu tư hoặc chủ trì thuê dịch vụ công nghệ thông tin.

- Hệ thống thông tin thuộc phạm vi quản lý của UBND cấp tỉnh gồm các hệ thống thông tin dùng chung, hệ thống thông tin phục vụ hoạt động nghiệp vụ và các hệ thống thông tin khác do các sở, ban, ngành, đơn vị sự nghiệp công lập, doanh nghiệp nhà nước, UBND cấp huyện và UBND cấp xã thuộc phạm vi quản lý của UBND tỉnh làm chủ đầu tư hoặc chủ trì thuê dịch vụ công nghệ thông tin.

Hệ thống thông tin phục vụ hoạt động quốc phòng, an ninh không thuộc phạm vi điều chỉnh của văn bản hướng dẫn này.

Việc xác định cấp độ; xây dựng, đề nghị thẩm định, trình phê duyệt Hồ sơ đề xuất cấp độ (HSĐXCĐ), cơ quan, tổ chức tham khảo tại Sổ tay hướng dẫn tuân thủ quy định pháp luật và tăng cường bảo đảm an toàn hệ thống thông tin theo cấp độ được ban hành kèm theo Công văn số 478/CATTT-ATHTTT ngày 30/3/2024 của Cục An toàn thông tin - Bộ Thông tin và Truyền thông.

III. TRIỂN KHAI CÁC BIỆN PHÁP BẢO VỆ THEO HỒ SƠ ĐỀ XUẤT CẤP ĐỘ ĐƯỢC PHÊ DUYỆT

3.1. Hướng dẫn chung

Hồ sơ đề xuất cấp độ đưa ra các phương án để đáp ứng các yêu cầu an toàn về quản lý và kỹ thuật theo quy định. Do đó, sau khi HSĐXCĐ được phê duyệt, cơ quan, tổ chức cần triển khai đầy đủ các biện pháp bảo đảm an toàn thông tin theo quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ trưởng Bộ Thông tin và Truyền thông.

Phương án bảo đảm an toàn thông tin về kỹ thuật đưa ra các yêu cầu về thiết kế, thiết lập hệ thống thông tin. Các yêu cầu kỹ thuật là cơ sở để cơ quan, tổ chức xác định được các biện pháp bảo đảm an toàn thông tin cần triển khai làm cơ sở để xác định các hạng mục cần bổ sung, đầu tư. Yêu cầu kỹ thuật cũng đưa ra yêu cầu về việc thiết lập cấu hình bảo mật trên từng thiết bị, máy chủ, ứng dụng và cơ sở dữ liệu trước khi đưa vào sử dụng.

Phương án bảo đảm an toàn thông tin về quản lý đưa ra các yêu cầu an toàn để bảo đảm an toàn hệ thống thông tin trong quá trình vận hành khai thác. Để đáp ứng các yêu cầu an toàn về quản lý, cơ quan, tổ chức cần xây dựng Quy chế bảo đảm an toàn thông tin. Trong đó, Quy chế bao gồm các quy định, quy trình bảo đảm an toàn thông tin nhằm đáp ứng toàn bộ các yêu cầu về quản lý theo quy định.

Việc triển khai phương án bảo đảm an toàn thông tin về quản lý và kỹ thuật, cơ quan, tổ chức có thể tham khảo hướng dẫn dưới đây.

3.2. Hướng dẫn triển khai các biện pháp về quản lý

Như đã hướng dẫn ở trên, cơ quan, tổ chức được khuyến nghị xây dựng và ban hành Quy chế bảo đảm an toàn thông tin. Trong đó, Quy chế bao gồm các quy định, quy trình bảo đảm an toàn thông tin nhằm đáp ứng toàn bộ các yêu cầu về quản lý theo quy định.

Quy chế bảo đảm an toàn thông tin do cấp có thẩm quyền ban hành, trước khi đưa hệ thống vào vận hành, khai thác theo quy định.

Quy chế bảo đảm an toàn thông tin cần quy định tối thiểu các nội dung sau để đáp ứng các yêu cầu an toàn về quản lý, bao gồm các nội dung:

1) Mục tiêu, nguyên tắc bảo đảm an toàn thông tin.

2) Phạm vi chính sách an toàn thông tin.

3) Quy định việc xây dựng, cập nhật và sửa đổi Quy chế.

4) Trách nhiệm bảo đảm an toàn thông tin.

5) Đầu mối phối hợp với cơ quan/tổ chức có thẩm quyền trong hoạt động bảo đảm an toàn thông tin.

6) Bảo đảm nguồn nhân lực.

Quy định chính sách/quy trình thực hiện quản lý bảo đảm nguồn nhân lực an toàn thông tin của tổ chức, bao gồm: Tuyển dụng cán bộ; quy chế/quy định bảo đảm an toàn thông tin trong quá trình làm việc và chấm dứt hoặc thay đổi công việc.

Các quy định đưa ra phải đáp ứng các yêu cầu về an toàn quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT và Tiêu chuẩn quốc gia TCVN 11930:2017 với tham chiếu tương ứng như dưới đây:

Cấp độ đề xuất	TCVN 11930:2017
Cấp độ 1	5.1.3
Cấp độ 2	6.1.3
Cấp độ 3	7.1.3
Cấp độ 4	8.1.3
Cấp độ 5	9.1.3

7) Quản lý thiết kế, xây dựng hệ thống.

Quy định chính sách/quy trình thực hiện quản lý thiết kế, xây dựng hệ thống của tổ chức, bao gồm: Thiết kế an toàn hệ thống thông tin; Phát triển phần mềm thuê khoán; Thử nghiệm và nghiệm thu hệ thống.

Các quy định đưa ra phải đáp ứng các yêu cầu về an toàn quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT và Tiêu chuẩn quốc gia TCVN 11930:2017 với tham chiếu tương ứng như dưới đây.

Cấp độ đề xuất	TCVN 11930:2017
Cấp độ 1	5.1.4
Cấp độ 2	6.1.4
Cấp độ 3	7.1.4
Cấp độ 4	8.1.4
Cấp độ 5	9.1.4

8) Quản lý vận hành hệ thống.

i) Quản lý an toàn mạng

Quy định chính sách/quy trình thực hiện quản lý an toàn hạ tầng mạng của tổ chức, bao gồm: Quản lý vận hành hoạt động bình thường của hệ thống; Cập nhật, sao lưu dự phòng và khôi phục hệ thống sau khi xảy ra sự cố; Truy cập và quản lý cấu hình hệ thống; Cấu hình tối ưu, tăng cường bảo mật cho thiết bị hệ thống (cứng hóa) trước khi đưa vào vận hành, khai thác.

Các quy định đưa ra phải đáp ứng các yêu cầu về an toàn quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT và Tiêu chuẩn quốc gia TCVN 11930:2017 với tham chiếu tương ứng như dưới đây.

Cấp độ đề xuất	TCVN 11930:2017
Cấp độ 1	5.1.5.1
Cấp độ 2	6.1.5.1
Cấp độ 3	7.1.5.1
Cấp độ 4	8.1.5.1
Cấp độ 5	9.1.5.1

ii) Quản lý an toàn máy chủ và ứng dụng

Quy định chính sách/quy trình thực hiện quản lý an toàn máy chủ và ứng dụng của tổ chức, bao gồm: Quản lý vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ; Truy cập mạng của máy chủ; Truy cập và quản trị máy chủ và ứng dụng; Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố; Cài đặt, gỡ bỏ hệ điều hành, dịch vụ, phần mềm trên hệ thống; Kết nối và gỡ bỏ hệ thống máy chủ và dịch vụ khỏi hệ thống; Cấu hình tối ưu và tăng cường bảo mật cho hệ thống máy chủ trước khi đưa vào vận hành, khai thác.

Các quy định đưa ra phải đáp ứng các yêu cầu về an toàn quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT và Tiêu chuẩn quốc gia TCVN 11930:2017 với tham chiếu tương ứng như dưới đây.

Cấp độ đề xuất	TCVN 11930:2017

Cấp độ 1	5.1.5.2
Cấp độ 2	6.1.5.2
Cấp độ 3	7.1.5.2
Cấp độ 4	8.1.5.2
Cấp độ 5	9.1.5.2

iii) Quản lý an toàn dữ liệu

Quy định chính sách/quy trình thực hiện quản lý an toàn dữ liệu của tổ chức, bao gồm: Yêu cầu an toàn đối với phương pháp mã hóa; Phân loại, quản lý và sử dụng khóa bí mật và dữ liệu mã hóa; Cơ chế mã hóa và kiểm tra tính nguyên vẹn của dữ liệu; Trao đổi dữ liệu qua môi trường mạng và phương tiện lưu trữ; Sao lưu dự phòng và khôi phục dữ liệu; Cập nhật đồng bộ thông tin, dữ liệu giữa hệ thống sao lưu dự phòng chính và hệ thống phụ.

Các quy định đưa ra phải đáp ứng các yêu cầu về an toàn quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT và Tiêu chuẩn quốc gia TCVN 11930:2017 với tham chiếu tương ứng như dưới đây.

Cấp độ đề xuất	**TCVN 11930:2017**
Cấp độ 1	5.1.5.3
Cấp độ 2	6.1.5.3
Cấp độ 3	7.1.5.3
Cấp độ 4	8.1.5.3
Cấp độ 5	9.1.5.3

iv) Quản lý an toàn thiết bị đầu cuối

Quy định chính sách/quy trình thực hiện quản lý an toàn thiết bị đầu cuối của tổ chức, bao gồm: Quản lý vận hành hoạt động bình thường cho thiết bị đầu cuối; Kết nối, truy cập và sử dụng thiết bị đầu cuối từ xa; Cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống; Cấu hình tối ưu và tăng cường bảo mật cho máy tính người sử dụng; Kiểm tra, đánh giá, xử lý điểm yếu an toàn thông tin cho thiết bị đầu cuối.

Các quy định đưa ra phải đáp ứng các yêu cầu về an toàn quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT và Tiêu chuẩn quốc gia TCVN 11930:2017 với tham chiếu tương ứng như dưới đây.

Cấp độ đề xuất	**TCVN 11930:2017**
Cấp độ 1	Không yêu cầu
Cấp độ 2	Không yêu cầu

Cấp độ 3	7.1.5.4
Cấp độ 4	8.1.5.4
Cấp độ 5	9.1.5.4

v) Quản lý phòng chống phần mềm độc hại

Quy định chính sách/quy trình thực hiện quản lý phòng chống phần mềm độc hại của tổ chức, bao gồm: Cài đặt, cập nhật, sử dụng phần mềm phòng chống mã độc; Cài đặt, sử dụng phần mềm trên máy tính, thiết bị di động và việc truy cập các trang thông tin trên mạng; Gửi nhận tập tin qua môi trường mạng và các phương tiện lưu trữ di động; Thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn bộ hệ thống; Kiểm tra và xử lý phần mềm độc hại.

Các quy định đưa ra phải đáp ứng các yêu cầu về an toàn quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT và Tiêu chuẩn quốc gia TCVN 11930:2017 với tham chiếu tương ứng như dưới đây.

Cấp độ đề xuất	**TCVN 11930:2017**
Cấp độ 1	Không yêu cầu
Cấp độ 2	Không yêu cầu
Cấp độ 3	7.1.5.5
Cấp độ 4	8.1.5.5
Cấp độ 5	9.1.5.5

vi) Quản lý giám sát an toàn hệ thống thông tin

Quy định chính sách/quy trình thực hiện quản lý giám sát an toàn hệ thống thông tin của tổ chức, bao gồm: Quản lý vận hành hoạt động bình thường của hệ thống giám sát; Đối tượng giám sát bao gồm; Kết nối và gửi nhật ký hệ thống; Truy cập và quản trị hệ thống giám sát; Loại thông tin cần được giám sát; Lưu trữ và bảo vệ thông tin giám sát; Theo dõi, giám sát và cảnh báo sự cố; Bố trí nguồn lực và tổ chức giám sát.

Các quy định đưa ra phải đáp ứng các yêu cầu về an toàn quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT và Tiêu chuẩn quốc gia TCVN 11930:2017 với tham chiếu tương ứng như dưới đây.

Cấp độ đề xuất	**TCVN 11930:2017**
Cấp độ 1	Không yêu cầu
Cấp độ 2	Không yêu cầu
Cấp độ 3	7.1.5.6
Cấp độ 4	8.1.5.6

Cấp độ 5	9.1.5.6

vii) Quản lý điểm yếu an toàn thông tin

Quy định chính sách/quy trình thực hiện quản lý điểm yếu an toàn thông tin của tổ chức, bao gồm: Quản lý thông tin các thành phần có trong hệ thống có khả năng tồn tại điểm yếu an toàn thông tin; Quản lý, cập nhật nguồn cung cấp điểm yếu an toàn thông tin; Phân nhóm và mức độ của điểm yếu; Cơ chế phối hợp với các nhóm chuyên gia; Kiểm tra, đánh giá và xử lý điểm yếu an toàn thông tin trước khi đưa hệ thống vào sử dụng; Quy trình khôi phục lại hệ thống.

Các quy định đưa ra phải đáp ứng các yêu cầu về an toàn quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT và Tiêu chuẩn quốc gia TCVN 11930:2017 với tham chiếu tương ứng như dưới đây.

Cấp độ đề xuất	**TCVN 11930:2017**
Cấp độ 1	Không yêu cầu
Cấp độ 2	Không yêu cầu
Cấp độ 3	7.1.5.7
Cấp độ 4	8.1.5.7
Cấp độ 5	9.1.5.7

viii) Quản lý sự cố an toàn thông tin

Quy định chính sách/quy trình thực hiện quản lý sự cố an toàn thông tin của tổ chức, bao gồm: Phân nhóm sự cố an toàn thông tin; Phương án tiếp nhận, phát hiện, phân loại và xử lý thông tin; Kế hoạch ứng phó sự cố an toàn thông tin; Giám sát, phát hiện và cảnh báo sự cố an toàn thông tin; Quy trình ứng cứu sự cố an toàn thông tin thông thường; Quy trình ứng cứu sự cố an toàn thông tin nghiêm trọng; Cơ chế phối hợp trong việc xử lý, khắc phục sự cố an toàn thông tin; Diễn tập phương án xử lý sự cố an toàn thông tin.

Các quy định đưa ra phải đáp ứng các yêu cầu về an toàn quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT và Tiêu chuẩn quốc gia TCVN 11930:2017 với tham chiếu tương ứng như dưới đây.

Cấp độ đề xuất	**TCVN 11930:2017**
Cấp độ 1	Không yêu cầu
Cấp độ 2	6.1.5.4
Cấp độ 3	7.1.5.8
Cấp độ 4	8.1.5.8
Cấp độ 5	9.1.5.8

ix) Quản lý an toàn người sử dụng đầu cuối

Quy định chính sách/quy trình thực hiện quản lý an toàn người sử dụng đầu cuối của tổ chức, bao gồm: Quản lý truy cập, sử dụng tài nguyên nội bộ; Quản lý truy cập mạng và tài nguyên trên Internet; Cài đặt và sử dụng máy tính an toàn.

Các quy định đưa ra phải đáp ứng các yêu cầu về an toàn quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT và Tiêu chuẩn quốc gia TCVN 11930:2017 với tham chiếu tương ứng như dưới đây.

Cấp độ đề xuất	TCVN 11930:2017
Cấp độ 1	Không yêu cầu
Cấp độ 2	6.1.5.5
Cấp độ 3	7.1.5.9
Cấp độ 4	8.1.5.9
Cấp độ 5	9.1.5.9

3.3. Hướng dẫn triển khai các biện pháp về kỹ thuật

Như đã hướng dẫn ở trên, để triển khai các biện pháp về kỹ thuật đáp ứng các yêu cầu an toàn theo quy định, các yêu cầu bao gồm các yêu cầu về thiết kế và thiết lập cấu hình bảo mật trên thiết bị hệ thống, máy chủ, ứng dụng và dữ liệu. Các yêu cầu liên quan đến thiết kế và phương án triển khai được hướng dẫn như dưới đây.

3.3.1. Thiết lập cấu hình bảo mật để đáp ứng các yêu cầu an toàn về thiết kế hệ thống

a) Quản lý truy cập, quản trị hệ thống từ xa an toàn

Thiết lập cấu hình cho sản phẩm VPN hoặc chức năng VPN được tích hợp trên tường lửa lớp mạng.

Một số biện pháp quản lý truy cập, quản trị hệ thống từ xa an toàn nâng cao cơ quan, tổ chức có thể tham khảo như: Cấu hình tính năng xác thực 2 lớp khi đăng nhập VPN; Thiết lập cấu hình VPN truy cập hệ thống thông qua máy chủ trung gian (Jump Server); Cấu hình chặn các IP nước ngoài truy cập đối với các hệ thống đặc thù…

Nhật ký hệ thống của sản phẩm/chức năng VPN được quản lý tập trung trên Hệ thống Quản lý và phân tích sự kiện an toàn thông tin (SIEM).

b) Quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập

Thiết lập cấu hình cho sản phẩm phòng chống xâm nhập hoặc chức năng phòng chống xâm nhập được tích hợp trên tường lửa lớp mạng.

Việc thiết lập cấu hình sản phẩm/chức năng phòng chống xâm nhập phải bảo đảm đầy đủ về độ phủ của các vùng mạng theo cấp độ tương ứng, bao gồm: Vùng mạng nội bộ; Vùng mạng biên; Vùng DMZ; Vùng máy chủ nội bộ; Vùng mạng không dây (nếu có) tách riêng, độc lập với các vùng mạng khác; Vùng mạng máy chủ cơ sở dữ liệu; Vùng quản trị; Vùng quản trị thiết bị hệ thống.

Nhật ký hệ thống của thiết bị/giải pháp được quản lý tập trung trên SIEM.

c) Cân bằng tải, dự phòng nóng cho các thiết bị mạng/thiết bị mạng chính

Thiết lập cấu hình chức năng cân bằng tải, dự phòng nóng trên thiết bị mạng/thiết bị mạng chính.

Các thiết bị mạng chính tối thiểu bao gồm: Thiết bị chuyển mạch trung tâm hoặc tương đương; Thiết bị tường lửa trung tâm; Tường lửa ứng dụng web; Hệ thống lưu trữ tập trung; Tường lửa cơ sở dữ liệu (nếu có).

d) Bảo đảm an toàn cho máy chủ cơ sở dữ liệu

Thiết lập cấu hình cho tường lửa cơ sở dữ liệu để bảo vệ cơ sở dữ liệu của hệ thống. Các cơ sở dữ liệu cần bảo vệ được xác định dựa vào Danh mục ứng dụng được đưa ra trong HSĐXCĐ.

Nhật ký hệ thống của tường lửa cơ sở dữ liệu được thiết lập và quản lý tập trung trên SIEM.

Đối với các hệ thống không yêu cầu bắt buộc sử dụng tường lửa cơ sở dữ liệu mà sử dụng phương án tương đương thì thiết lập cấu hình hệ thống như sau:

- Thiết lập cấu hình tường lửa Hệ điều hành máy chủ cơ sở dữ liệu để quản lý truy cập giữa các máy chủ trong cùng một vùng mạng.

- Thực hiện cấu hình tăng cường bảo mật cho Hệ điều hành và Cơ sở dữ liệu. Cơ quan, tổ chức có thể tham khảo tài liệu SP800-123 Guide to General Server Security của Viện Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ - NIST để thực hiện.

- Thiết lập cấu hình hệ thống để toàn bộ hoạt động liên quan đến cơ sơ dữ liệu được quản lý trên Hệ thống SIEM.

- Thiết lập cấu hình hệ thống để định kỳ tự động thực hiện sao lưu dự phòng cơ sở dữ liệu trên hệ thống lưu trữ độc lập.

đ) Chặn lọc phần mềm độc hại trên môi trường mạng

Thiết lập cấu hình cho sản phẩm hoặc chức năng phòng, chống mã độc trên môi trường mạng được tích hợp trên tường lửa lớp mạng/thiết bị phòng, chống xâm nhập.

Việc thiết lập cấu hình phòng, chống mã độc trên môi trường mạng phải bảo đảm đầy đủ về độ phủ của các vùng mạng theo cấp độ tương ứng, bao gồm:

Vùng mạng nội bộ; Vùng mạng biên; Vùng DMZ; Vùng máy chủ nội bộ; Vùng mạng không dây (nếu có) tách riêng, độc lập với các vùng mạng khác; Vùng mạng máy chủ cơ sở dữ liệu; Vùng quản trị; Vùng quản trị thiết bị hệ thống.

Nhật ký hệ thống của sản phẩm được thiết lập và quản lý tập trung trên SIEM.

e) Phòng chống tấn công từ chối dịch vụ

Thiết lập cấu hình trên sản phẩm phòng chống tấn công từ chối dịch vụ hoặc có giải pháp tương đương hoặc thuê dịch vụ chuyên nghiệp của doanh nghiệp để phòng, chống tấn công từ chối dịch vụ lớp ứng dụng và lớp mạng.

Nhật ký hệ thống của sản phẩm được thiết lập và quản lý tập trung trên SIEM.

g) Phòng chống tấn công mạng cho ứng dụng web

Thiết lập cấu hình cho sản phẩm tường lửa ứng dụng web để bảo vệ toàn bộ ứng dụng (theo Danh mục ứng dụng được đưa ra trong HSĐXCĐ) của hệ thống, được cung cấp dịch vụ ra bên ngoài.

Tường lửa ứng dụng web là thiết bị mạng chính, do đó cần cấu hình chức năng cân bằng tải, dự phòng nóng cho thiết bị này.

Nhật ký hệ thống của sản phẩm này được thiết lập và quản lý tập trung trên SIEM.

Đối với các hệ thống không yêu cầu bắt buộc sử dụng tường lửa ứng dụng web mà sử dụng phương án tương đương thì thiết lập cấu hình hệ thống như sau:

- Thiết lập Máy chủ đại diện (Reverse proxy) và có kiểm soát truy cập và phòng chống xâm nhập giữa máy chủ đại diện và máy chủ ứng dụng web.
- Thiết lập cấu hình tăng cường bảo mật cho máy chủ Reverse proxy, cài đặt phần mềm phòng, chống phần mềm độc hại.
- Thiết lập cấu hình tường lửa trên máy chủ Reverse proxy.
- Kiểm tra, đánh giá an toàn thông tin cho máy chủ Reverse proxy.

h) Bảo đảm an toàn thông tin cho hệ thống thư điện tử

Thiết lập cấu hình trên sản phẩm bảo đảm an toàn thông tin cho hệ thống thư điện tử để bảo vệ hệ thống thư điện tử.

Nhật ký hệ thống của sản phẩm được thiết lập và quản lý tập trung trên SIEM.

i) Quản lý truy cập lớp mạng

Thiết lập cấu hình cho sản phẩm quản lý truy cập lớp mạng để quản lý thông tin, truy cập của máy chủ, máy trạm và thiết bị hệ thống trong mạng.

Nhật ký hệ thống của sản phẩm được thiết lập và quản lý tập trung trên SIEM.

Đối với các hệ thống thông tin không yêu cầu sử dụng sản phẩm quản lý truy cập lớp mạng thì thiết lập cấu hình hệ thống tương đương đáp ứng tối thiểu các yêu cầu sau:

- Thiết lập cấu hình bảo mật trên thiết bị chuyển mạch lớp 2 cho phép phát hiện và quản lý truy cập mạng lớp 2 đối với các thiết bị kết nối vào hệ thống.

- Thiết lập cấu hình nhật ký hệ thống trên thiết bị lớp 2 để quản lý được thông tin kết nối của các thiết bị vào hệ thống SIEM.

k) Giám sát hệ thống thông tin tập trung

Thiết lập cấu hình trên sản phẩm/giải pháp giám sát hệ thống thông tin tập trung đáp ứng tối thiểu các yêu cầu sau:

- Giám sát được trạng thái hoạt động của thiết bị, máy chủ và ứng dụng được thuyết minh trong HSĐXCĐ; Cấu hình các chức năng cảnh báo bất thường, ảnh hưởng tới hoạt động bình thường của thiết bị, máy chủ và ứng dụng qua tin nhắn, thư điện tử…

- Trạng thái giám sát tối thiểu bao gồm các thông tin hiệu năng của CPU, RAM, Storage và các giao diện mạng.

l) Giám sát an toàn hệ thống thông tin tập trung

Thiết lập cấu hình trên sản phẩm SIEM hoặc sản phẩm có chức năng tương đương để quản lý tập trung nhật ký hệ thống của thiết bị hệ thống, máy chủ, máy trạm, ứng dụng và các thành phần khác của hệ thống (nếu có).

Danh mục các thiết bị hệ thống, máy chủ, máy trạm, ứng dụng được đưa ra trong HSĐXCĐ.

Một số yêu cầu tối thiểu đối với hệ thống SIEM bao gồm:

- Có chức năng quản trị: Chức năng phân tích tương quan (Correlation), Chức năng lọc (Filters), Tạo các luật (Rules), Chức năng hiển thị (Dashboards), Chức năng cảnh báo và báo cáo (Alerts and Reports), Chức năng cảnh báo thời gian thực (Real Time Alert).

- Có chức năng nhận log: Cho phép nhận log từ các nguồn với nhiều định dạng khác nhau từ các thiết bị mạng, máy chủ và ứng dụng; định dạng, chuẩn hóa log nhận được theo các trường thông tin tùy biến theo nhu cầu sử dụng.

m) Quản lý sao lưu dự phòng tập trung

Thiết lập cấu hình trên hệ thống quản lý sao lưu dự phòng tập trung để quản lý sao lưu dự phòng tập trung, sử dụng giải pháp như SAN, NAS…

Việc thiết lập cấu hình trên hệ thống quản lý sao lưu dự phòng tập trung cần đáp ứng tối thiểu các yêu cầu sau:

- Tối thiểu các dữ liệu sau yêu cầu được lưu trữ trên hệ thống quản lý tập trung: Ảnh hệ điều hành của các máy chủ trong hệ thống, tệp tin cấu hình các thiết bị hệ thống, cơ sở dữ liệu và dữ liệu nghiệp vụ (nếu có).

n) Quản lý phần mềm phòng chống mã độc trên các máy chủ/máy tính người dùng tập trung

Thiết lập cấu hình hệ thống quản lý phần mềm phòng chống mã độc đáp ứng tối thiểu các yêu cầu:

- Có chức năng quản lý tập trung.

- Toàn bộ các máy chủ, máy trạm trong hệ thống được cài đặt sản phẩm và được quản lý trên hệ thống quản lý tập trung. Đối với các máy chủ chuyên dụng mà không có sản phẩm phòng chống mã độc trên thị trường hỗ trợ thì cần có phương án tương đương để hỗ trợ phòng, chống mã độc như: phòng, chống mã độc trên môi trường mạng; cấu hình tăng cường bảo mật…

o) Phòng, chống thất thoát dữ liệu

Thiết lập cấu hình sản phẩm, giải pháp Phòng, chống thất thoát dữ liệu đáp ứng tối thiểu các máy chủ cơ sở dữ liệu, máy tính quản trị cơ sở dữ liệu, máy tính phục vụ hoạt động nghiệp vụ xử lý dữ liệu được triển khai các giải pháp phòng, chống thất thoát dữ liệu.

Đối với các hệ thống thông tin không yêu cầu sử dụng sản phẩm Phòng, chống thất thoát dữ liệu thì hệ thống cần được thiết lập đáp ứng tối thiểu các yêu cầu sau:

- Sử dụng chức năng phòng, chống thất thoát dữ liệu được tích hợp trên thiết bị/sản phẩm bảo mật sử dụng trong hệ thống (nếu có).

- Thiết lập cấu hình tường lửa Hệ điều hành máy chủ cơ sở dữ liệu để quản lý truy cập giữa các máy chủ trong cùng một vùng mạng.

- Cấu hình tăng cường bảo mật cho Hệ điều hành và Cơ sở dữ liệu.

- Cấu hình tăng cường bảo mật cho các máy tính quản trị cơ sở dữ liệu, máy tính phục vụ hoạt động nghiệp vụ xử lý dữ liệu.

p) Dự phòng kết nối mạng Internet cho các máy chủ dịch vụ

Thiết lập cấu hình hệ thống để dự phòng kết nối mạng Internet cho các máy chủ dịch vụ.

Khuyến nghị sử dụng phương án duy trì 02 kết nối Internet của hai nhà cung cấp khác nhau. Hệ thống có dải địa chỉ IP Public và có số hiệu mạng ASN riêng khi kết nối định tuyến với các nhà cung cấp khác nhau.

q) Phương án bảo đảm an toàn cho mạng không dây

Thiết lập cấu hình hệ thống để bảo mật cho mạng không dây sử dụng giải pháp chuyên dụng hoặc việc thiết lập cấu hình bảo mật trên hệ thống để bảo đảm an toàn cho mạng không dây.

x) Phương án quản lý tài khoản đặc quyền

Thiết lập cấu hình sản phẩm/giải pháp quản lý tài khoản đặc quyền cho phép quản lý tập trung việc xác thực, phân quyền, giám sát hành vi và các chức năng bảo mật khác để quản lý các tài khoản quản trị trong hệ thống.

Nhật ký hệ thống của sản phẩm/giải pháp được thiết lập và quản lý tập trung trên SIEM.

y) Dự phòng hệ thống ở vị trí địa lý khác nhau

Hệ thống ở vị trí địa lý khác nhau, cách nhau tối thiểu 30 km.

z) Dự phòng cho kết nối mạng giữa hệ thống chính và hệ thống dự phòng

Thiết lập cấu hình trên thiết bị hệ thống để kết nối mạng giữa hệ thống chính và hệ thống dự phòng để thực hiện đồng bộ dữ liệu và dự phòng nóng khi hệ thống chính xảy ra sự cố.

3.3.2. Thiết lập cấu hình thiết bị hệ thống

a) Kiểm soát truy cập từ bên ngoài mạng

Thiết lập cấu hình trên thiết bị hệ thống để quản lý truy cập từ các mạng bên ngoài theo chiều đi vào hệ thống tới các máy chủ dịch vụ bên trong mạng, bao gồm: Các dịch vụ/ứng dụng cho phép truy cập từ bên ngoài; Thời gian mất kết nối; Phân quyền truy cập; Giới hạn kết nối; Thiết lập chính sách ưu tiên. Phương án cần mô tả chính sách đó được thiết lập trên thiết bị hệ thống nào.

Thiết lập cấu hình trên thiết bị hệ thống phải đáp ứng các yêu cầu về an toàn quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT và Tiêu chuẩn quốc gia TCVN 11930:2017 với tham chiếu tương ứng như dưới đây.

Cấp độ đề xuất	**TCVN 11930:2017**
Cấp độ 1	5.2.1.2
Cấp độ 2	6.2.1.2
Cấp độ 3	7.2.1.2
Cấp độ 4	8.2.1.2
Cấp độ 5	9.2.1.2

b) Kiểm soát truy cập từ bên trong mạng

Thiết lập cấu hình trên thiết bị hệ thống để quản lý truy cập từ các máy tính/máy chủ bên trong mạng theo chiều đi ra các mạng bên ngoài và các mạng khác bên trong mạng, bao gồm: Các ứng dụng/dịch vụ nào được truy cập; Quản lý truy cập theo địa chỉ thiết bị; Phương án ưu tiên truy cập. Phương án cần mô tả chính sách đó được thiết lập trên thiết bị hệ thống nào.

Thiết lập cấu hình trên thiết bị hệ thống phải đáp ứng các yêu cầu về an toàn quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT và Tiêu chuẩn quốc gia TCVN 11930:2017 với tham chiếu tương ứng như dưới đây.

Cấp độ đề xuất	**TCVN 11930:2017**
Cấp độ 1	Không yêu cầu
Cấp độ 2	6.2.1.3
Cấp độ 3	7.2.1.3
Cấp độ 4	8.2.1.3
Cấp độ 5	9.2.1.3

c) Nhật ký hệ thống

Thiết lập cấu hình trên thiết bị hệ thống để quản lý nhật ký hệ thống (log) trên các thiết bị hệ thống về bật chức năng ghi log; thông tin ghi log; thời gian, dung lượng ghi log; quản lý log.

Thiết lập cấu hình trên thiết bị hệ thống phải đáp ứng các yêu cầu về an toàn quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT và Tiêu chuẩn quốc gia TCVN 11930:2017 với tham chiếu tương ứng như dưới đây.

Cấp độ đề xuất	**TCVN 11930:2017**
Cấp độ 1	5.2.1.3
Cấp độ 2	6.2.1.4
Cấp độ 3	7.2.1.4
Cấp độ 4	8.2.1.4
Cấp độ 5	9.2.1.4

d) Phòng chống xâm nhập

Thiết lập cấu hình trên thiết bị phòng, chống xâm nhập IDS/IPS hoặc chức năng IDS/IPS trên thiết bị tường lửa có trong hệ thống, đáp ứng các yêu cầu về an toàn quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT và Tiêu chuẩn quốc gia TCVN 11930:2017 với tham chiếu tương ứng như dưới đây.

Cấp độ đề xuất	TCVN 11930:2017
Cấp độ 1	5.2.1.4
Cấp độ 2	6.2.1.5
Cấp độ 3	7.2.1.5
Cấp độ 4	8.2.1.5
Cấp độ 5	9.2.1.5

d) Phòng chống phần mềm độc hại trên môi trường mạng

Thiết lập cấu hình trên thiết bị hệ thống để thực hiện chức năng phòng chống phần mềm độc hại trên môi trường mạng, đáp ứng các yêu cầu về an toàn quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT và Tiêu chuẩn quốc gia TCVN 11930:2017 với tham chiếu tương ứng như dưới đây.

Cấp độ đề xuất	TCVN 11930:2017
Cấp độ 1	Không yêu cầu
Cấp độ 2	Không yêu cầu
Cấp độ 3	7.2.1.6
Cấp độ 4	8.2.1.6
Cấp độ 5	9.2.1.6

đ) Bảo vệ thiết bị hệ thống

Thiết lập cấu hình trên thiết bị hệ thống để bảo đảm bảo đảm an toàn cho thiết bị trong quá trình sử dụng và quản lý vận hành, đáp ứng các yêu cầu về an toàn quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT và Tiêu chuẩn quốc gia TCVN 11930:2017 với tham chiếu tương ứng như dưới đây.

Cấp độ đề xuất	TCVN 11930:2017
Cấp độ 1	5.2.1.5
Cấp độ 2	6.2.1.6
Cấp độ 3	7.2.1.7
Cấp độ 4	8.2.1.7
Cấp độ 5	9.2.1.7

3.3.3. Thiết lập cấu hình bảo mật cho máy chủ

a) Xác thực

Thiết lập cấu hình chức năng xác thực trên máy chủ để bảo đảm việc xác thực khi đăng nhập vào máy chủ an toàn.

Thiết lập cấu hình trên máy chủ phải đáp ứng các yêu cầu về an toàn quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT và Tiêu chuẩn quốc gia TCVN 11930:2017 với tham chiếu tương ứng như dưới đây.

Cấp độ đề xuất	TCVN 11930:2017
Cấp độ 1	5.2.2.1
Cấp độ 2	6.2.2.1
Cấp độ 3	7.2.2.1
Cấp độ 4	8.2.2.1
Cấp độ 5	9.2.2.1

b) Kiểm soát truy cập

Thiết lập cấu hình chức năng kiểm soát truy cập trên máy chủ để bảo đảm việc truy cập, sử dụng máy chủ an toàn sau khi đăng nhập thành công.

Thiết lập cấu hình trên máy chủ phải đáp ứng các yêu cầu về an toàn quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT và Tiêu chuẩn quốc gia TCVN 11930:2017 với tham chiếu tương ứng như dưới đây.

Cấp độ đề xuất	TCVN 11930:2017
Cấp độ 1	5.2.2.2
Cấp độ 2	6.2.2.2
Cấp độ 3	7.2.2.2
Cấp độ 4	8.2.2.2
Cấp độ 5	9.2.2.2

c) Nhật ký hệ thống

Thiết lập cấu hình chức năng ghi nhật ký hệ thống (log) trên các máy chủ về: Bật chức năng ghi log; Thông tin ghi log; Thời gian, Dung lượng ghi log; Quản lý log.

Thiết lập cấu hình trên máy chủ phải đáp ứng các yêu cầu về an toàn quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT và Tiêu chuẩn quốc gia TCVN 11930:2017 với tham chiếu tương ứng như dưới đây.

Cấp độ đề xuất	TCVN 11930:2017
Cấp độ 1	5.2.2.3
Cấp độ 2	6.2.2.3
Cấp độ 3	7.2.2.3
Cấp độ 4	8.2.2.3

Cấp độ 5	9.2.2.3

d) Phòng chống xâm nhập

Thiết lập cấu hình bảo mật trên máy chủ để bảo bảo vệ tấn công xâm nhập từ bên ngoài.

Thiết lập cấu hình trên máy chủ phải đáp ứng các yêu cầu về an toàn quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT và Tiêu chuẩn quốc gia TCVN 11930:2017 với tham chiếu tương ứng như dưới đây.

Cấp độ đề xuất	**TCVN 11930:2017**
Cấp độ 1	5.2.2.4
Cấp độ 2	6.2.2.4
Cấp độ 3	7.2.2.4
Cấp độ 4	8.2.2.4
Cấp độ 5	9.2.2.4

đ) Phòng chống phần mềm độc hại

Thiết lập cấu hình chức năng phòng, chống mã độc trên máy chủ về: Cài đặt phần mềm phòng chống mã độc; Dò quét mã độc; Xử lý mã độc; Quản lý tập trung phần mềm phòng chống mã độc... để phòng chống mã độc cho máy chủ.

Thiết lập cấu hình trên máy chủ phải đáp ứng các yêu cầu về an toàn quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT và Tiêu chuẩn quốc gia TCVN 11930:2017 với tham chiếu tương ứng như dưới đây.

Cấp độ đề xuất	**TCVN 11930:2017**
Cấp độ 1	5.2.2.5
Cấp độ 2	6.2.2.5
Cấp độ 3	7.2.2.5
Cấp độ 4	8.2.2.5
Cấp độ 5	9.2.2.5

e) Xử lý máy chủ khi chuyển giao

Mô tả phương án kỹ thuật, công cụ để cho phép xóa sạch dữ liệu; sao lưu dự phòng dữ liệu khi chuyển giao hoặc thay đổi mục đích sử dụng.

Thiết lập cấu hình trên máy chủ phải đáp ứng các yêu cầu về an toàn quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT và Tiêu chuẩn quốc gia TCVN 11930:2017 với tham chiếu tương ứng như dưới đây.

Cấp độ đề xuất	**TCVN 11930:2017**

Cấp độ 1	Không yêu cầu
Cấp độ 2	6.2.2.6
Cấp độ 3	7.2.2.6
Cấp độ 4	8.2.2.6
Cấp độ 5	9.2.2.6

3.3.4. Thiết lập cấu hình bảo mật cho ứng dụng

a) Xác thực

Thiết lập cấu hình chức năng xác thực trên ứng dụng để bảo đảm việc xác thực khi đăng nhập vào ứng dụng an toàn.

Thiết lập cấu hình trên ứng dụng phải đáp ứng các yêu cầu về an toàn quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT và Tiêu chuẩn quốc gia TCVN 11930:2017 với tham chiếu tương ứng như dưới đây.

Cấp độ đề xuất	**TCVN 11930:2017**
Cấp độ 1	5.2.3.1
Cấp độ 2	6.2.3.1
Cấp độ 3	7.2.3.1
Cấp độ 4	8.2.3.1
Cấp độ 5	9.2.3.1

b) Kiểm soát truy cập

Thiết lập cấu hình chức năng kiểm soát truy cập trên ứng dụng để bảo đảm việc truy cập, sử dụng ứng dụng an toàn sau khi đăng nhập thành công.

Thiết lập cấu hình trên ứng dụng phải đáp ứng các yêu cầu về an toàn quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT và Tiêu chuẩn quốc gia TCVN 11930:2017 với tham chiếu tương ứng như dưới đây.

Cấp độ đề xuất	**TCVN 11930:2017**
Cấp độ 1	5.2.3.2
Cấp độ 2	6.2.3.2
Cấp độ 3	7.2.3.2
Cấp độ 4	8.2.3.2
Cấp độ 5	9.2.3.2

c) Nhật ký hệ thống

Thiết lập cấu hình chức năng ghi nhật ký hệ thống (log) trên các ứng dụng về: Bật chức năng ghi log; Thông tin ghi log; Thời gian, dung lượng ghi log; Quản lý log.

Thiết lập cấu hình trên ứng dụng phải đáp ứng các yêu cầu về an toàn quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT và Tiêu chuẩn quốc gia TCVN 11930:2017 với tham chiếu tương ứng như dưới đây.

Cấp độ đề xuất	**TCVN 11930:2017**
Cấp độ 1	5.2.3.3
Cấp độ 2	6.2.3.3
Cấp độ 3	7.2.3.3
Cấp độ 4	8.2.3.3
Cấp độ 5	9.2.3.3

d) Bảo mật thông tin liên lạc

Thiết lập cấu hình trên ứng dụng để mã hóa và sử dụng giao thức mạng hoặc kênh kết nối mạng an toàn khi trao đổi dữ liệu qua môi trường mạng.

Thiết lập cấu hình trên ứng dụng phải đáp ứng các yêu cầu về an toàn quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT và Tiêu chuẩn quốc gia TCVN 11930:2017 với tham chiếu tương ứng như dưới đây.

Cấp độ đề xuất	**TCVN 11930:2017**
Cấp độ 1	Không yêu cầu
Cấp độ 2	Không yêu cầu
Cấp độ 3	7.2.3.4
Cấp độ 4	8.2.3.4
Cấp độ 5	9.2.3.4

e) Chống chối bỏ

Thiết lập cấu hình trên ứng dụng để sử dụng và bảo vệ chữ ký số để bảo vệ tính bí mật và chống chối bỏ khi gửi/nhận thông tin quan trọng qua mạng.

Thiết lập cấu hình trên ứng dụng phải đáp ứng các yêu cầu về an toàn quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT và Tiêu chuẩn quốc gia TCVN 11930:2017 với tham chiếu tương ứng như dưới đây.

Cấp độ đề xuất	**TCVN 11930:2017**
Cấp độ 1	Không yêu cầu

Cấp độ 2	Không yêu cầu
Cấp độ 3	7.2.3.5
Cấp độ 4	8.2.3.5
Cấp độ 5	9.2.3.5

g) An toàn ứng dụng và mã nguồn

Cấu hình/thiết lập chức năng bảo mật cho ứng dụng và phương án bảo vệ mã nguồn ứng dụng đáp ứng các yêu cầu về an toàn quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT và Tiêu chuẩn quốc gia TCVN 11930:2017 với tham chiếu tương ứng như dưới đây.

Cấp độ đề xuất	**TCVN 11930:2017**
Cấp độ 1	Không yêu cầu
Cấp độ 2	6.2.3.4
Cấp độ 3	7.2.3.6
Cấp độ 4	8.2.3.6
Cấp độ 5	9.2.3.6

3.3.5. Thiết lập cấu hình bảo mật cho dữ liệu

a) Nguyên vẹn dữ liệu

Thiết lập cấu hình trên hệ thống lưu trữ để lưu trữ, quản lý thay đổi, khôi phục dữ liệu bảo đảm tính nguyên vẹn của dữ liệu.

Thiết lập cấu hình trên hệ thống lưu trữ phải đáp ứng các yêu cầu về an toàn quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT và Tiêu chuẩn quốc gia TCVN 11930:2017 với tham chiếu tương ứng như dưới đây.

Cấp độ đề xuất	**TCVN 11930:2017**
Cấp độ 1	Không yêu cầu
Cấp độ 2	Không yêu cầu
Cấp độ 3	7.2.4.1
Cấp độ 4	8.2.4.1
Cấp độ 5	9.2.4.1

b) Bảo mật dữ liệu

Thiết lập cấu hình trên hệ thống lưu trữ để lưu trữ, quản lý thay đổi, khôi phục dữ liệu bảo đảm tính bí mật của dữ liệu.

Thiết lập cấu hình trên hệ thống lưu trữ phải đáp ứng các yêu cầu về an toàn quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT và Tiêu chuẩn quốc gia TCVN 11930:2017 với tham chiếu tương ứng như dưới đây.

Cấp độ đề xuất	**TCVN 11930:2017**
Cấp độ 1	Không yêu cầu
Cấp độ 2	6.2.4.1
Cấp độ 3	7.2.4.2
Cấp độ 4	8.2.4.2
Cấp độ 5	9.2.4.2

c) Sao lưu dự phòng

Thiết lập cấu hình trên hệ thống lưu trữ để sao lưu dự phòng dữ liệu: Các thông tin yêu cầu sao lưu dự phòng; Phân loại dữ liệu sao lưu dự phòng; Hệ thống sao lưu dự phòng…

Thiết lập cấu hình trên hệ thống lưu trữ phải đáp ứng các yêu cầu về an toàn quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT và Tiêu chuẩn quốc gia TCVN 11930:2017 với tham chiếu tương ứng như dưới đây.

Cấp độ đề xuất	**TCVN 11930:2017**
Cấp độ 1	5.2.4.1
Cấp độ 2	6.2.4.2
Cấp độ 3	7.2.4.3
Cấp độ 4	8.2.4.3
Cấp độ 5	9.2.4.3

IV. TỔ CHỨC BẢO ĐẢM AN TOÀN THEO MÔ HÌNH 4 LỚP

4.1. Hướng dẫn chung

Hệ thống thông tin sau khi được phê duyệt Hồ sơ đề xuất cấp độ, cần được triển khai đầy đủ phương án bảo đảm an toàn thông tin bao gồm: thiết kế, thiết lập hệ thống; quản lý, vận hành hệ thống theo Quy chế bảo đảm an toàn thông tin được ban hành cùng Hồ sơ đề xuất cấp độ.

Để triển khai phương án bảo đảm an toàn hệ thống thông tin một cách tổng thể, đồng bộ và hiệu quả, cơ quan tổ chức cần tổ chức triển khai toàn diện, thực chất công tác bảo đảm an toàn thông tin theo mô hình 4 lớp.

Tổ chức triển khai toàn diện, thực chất công tác bảo đảm an toàn thông tin theo mô hình 4 lớp là việc triển khai đầy đủ 4 lớp bảo vệ bao gồm: (1) Lực lượng tại chỗ; (2) Tổ chức hoặc doanh nghiệp giám sát, bảo vệ chuyên nghiệp; (3) Tổ chức hoặc doanh nghiệp độc lập kiểm tra, đánh giá định kỳ; (4) Kết nối, chia sẻ thông tin với hệ thống giám sát quốc gia.

Trong đó, việc Tổ chức hoặc doanh nghiệp giám sát, bảo vệ chuyên nghiệp (Lớp 2) thực hiện đầy đủ bao gồm: (1) Lớp mạng, (2) Lớp Máy chủ, (3) Lớp ứng dụng, (4) Lớp thiết bị đầu cuối. Tổ chức hoặc doanh nghiệp độc lập kiểm tra, đánh giá định kỳ thực hiện đầy đủ (Lớp 3) thực hiện đầy đủ, bao gồm: Thiết bị hệ thống; Máy chủ và Ứng dụng.

Trên cơ sở đó, Bộ Thông tin và Truyền thông xây dựng Tài liệu này để hướng dẫn các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân cấp tỉnh triển khai toàn diện, thực chất công tác bảo đảm an toàn thông tin theo mô hình 4 lớp đối với các hệ thống thông tin thuộc phạm vi quản lý.

4.2. Lực lượng tại chỗ - Lớp 1

Lực lượng tại chỗ là lớp thứ nhất trong tổ chức bảo đảm an toàn thông tin theo mô hình 4 lớp. Lớp này giúp cơ quan, tổ chức kiện toàn lực lượng tại chỗ và nâng cao năng lực của cán bộ chuyên trách để triển khai các lớp tiếp theo của Mô hình 4 lớp.

Nội dung triển khai Lớp 1. Lực lượng tại chỗ bao gồm các nội dung: (1) Kiện toàn lực lượng tại chỗ; (2) Nâng cao năng lực; (3) Mạng lưới.

4.2.1. Kiện toàn lực lượng tại chỗ

Một số nội dung trọng tâm cơ quan, tổ chức cần triển khai để kiện toàn lực lượng tại chỗ bao gồm:

a) Người đứng đầu cơ quan, tổ chức trực tiếp chỉ đạo, trong trường hợp cần thiết có thể giao thêm 01 Lãnh đạo cấp phó của mình đảm nhận nhiệm vụ thường trực, giúp Người đứng đầu;

b) Người đứng đầu đơn vị chuyên trách trực tiếp chỉ đạo, trong trường hợp cần thiết có thể giao thêm 01 Lãnh đạo cấp phó của mình đảm nhận nhiệm vụ thường trực, giúp Người đứng đầu;

c) Chỉ định bộ phận chuyên trách về an toàn thông tin thuộc đơn vị chuyên trách về công nghệ thông tin, trong trường hợp chưa có đơn vị chuyên trách về an toàn thông tin độc lập;

d) Thành lập Tổ/Đội bảo đảm an toàn, an ninh mạng/Ứng cứu sự cố liên ngành theo hướng chuyên nghiệp, cơ động với sự tham gia của đại diện các cơ quan, tổ chức trực thuộc do đơn vị chuyên trách làm thường trực.

4.2.2. Nâng cao năng lực

Một số nội dung trọng tâm cơ quan, tổ chức cần triển khai để nâng cao năng lực tại chỗ bao gồm:

a) Khuyến nghị bố trí tối thiểu 05 chuyên gia an toàn thông tin mạng (bao gồm cả chuyên gia thuê ngoài) đáp ứng chuẩn kỹ năng về an toàn thông tin do Bộ Thông tin và Truyền thông quy định tại Thông tư 17/2021/TT-BTTTT ngày 30/11/2021.

b) Xây dựng kế hoạch và tổ chức đào tạo chuyên sâu về an toàn thông tin cho nhân sự chuyên trách; hàng năm tổ chức đào tạo, tuyên truyền tới toàn thể cán bộ, công chức, viên chức, người lao động thuộc phạm vi quản lý theo chỉ đạo của Thủ tướng Chính phủ tại Quyết định số 21/QĐ-TTg ngày 06/11/2021.

c) Xây dựng kế hoạch và hàng năm tổ chức tuyên truyền, nâng cao nhận thức và phổ biến kiến thức về an toàn thông tin tới toàn thể cán bộ, công chức, viên chức, người lao động thuộc phạm vi quản lý theo chỉ đạo của Thủ tướng Chính phủ tại Quyết định số 1907/QĐ-TTg ngày 23/11/2020.

d) Tổ chức diễn tập thực chiến tối thiểu 01 lần/năm đối với hệ thống thông tin cấp độ 3 trở lên theo chỉ đạo của Thủ tướng Chính phủ tại Quyết định số 18/CT-TTg ngày 13/10/2022.

đ) Tăng cường sử dụng và khai thác hiệu quả các nền tảng hỗ trợ bảo đảm an toàn thông tin do Bộ Thông tin và Truyền thông cung cấp, gồm: Nền tảng hỗ trợ quản lý bảo đảm an toàn hệ thống thông tin theo cấp độ (https://capdo.ais.gov.vn); Nền tảng điều phối xử lý sự cố an toàn thông tin mạng quốc gia (https://irlab.vn); Nền tảng hỗ trợ điều tra số (https://df.irlab.vn).

Hướng dẫn sử dụng chi tiết các Nền tảng tại Mục V văn bản này.

4.2.3. Mạng lưới

Đăng ký tham gia mạng lưới do Trung tâm VNCERT/CC, Cục An toàn thông tin làm điều phối.

4.3. Giám sát bảo vệ - Lớp 2

4.3.1. Hướng dẫn chung về giám sát, bảo vệ - Lớp 2

Giám sát, bảo vệ chuyên nghiệp là lớp thứ 2 trong Mô hình 4 lớp giúp cơ quan, tổ chức triển khai giải pháp giám sát, bảo vệ chuyên nghiệp cho các hệ thống thông tin thuộc phạm vi quản lý.

Một số điểm cơ quan, tổ chức cần lưu ý khi triển khai lớp giám sát, bảo vệ như sau:

- Mỗi hệ thống thông tin được xác định, phê duyệt đầy đủ các biện pháp bảo đảm an toàn hệ thống thông tin theo cấp độ. Việc triển khai Lớp 2 giám sát bảo vệ hệ thống thông tin là việc tổ chức triển khai các giải pháp nhằm đáp ứng đầy đủ các yêu cầu an toàn theo phương án được phê duyệt trong Hồ sơ đề xuất cấp độ.

- Bảo đảm về độ rộng và sâu khi triển khai giám sát, bảo vệ. Trong đó độ rộng bảo đảm toàn bộ hệ thống thông tin thuộc phạm vi quản lý được giám sát (cấp Xã, Huyện, Sở, ban, ngành đối với địa phương; các đơn vị Cục, Vụ, Trung tâm, ban quản lý… đối với các bộ, ngành); độ sâu là bảo đảm đầy đủ (1) Lớp Mạng; (2) Lớp Máy chủ; (3) Lớp Ứng dụng; (4) Lớp Thiết bị đầu cuối.

- Trong trường hợp nguồn lực hạn chế thì về độ rộng cần ưu tiên các hệ thống thông tin có cấp độ an toàn hệ thống thông tin cao trước; các hệ thống thông tin dùng chung hoặc các hệ thống cơ sở hạ tầng thông tin. Hệ thống thông tin cấp độ 3 trở lên yêu cầu giám sát đầy đủ (1) Lớp Mạng; (2) Lớp Máy chủ; (3) Lớp Ứng dụng; (4) Lớp Thiết bị đầu cuối.

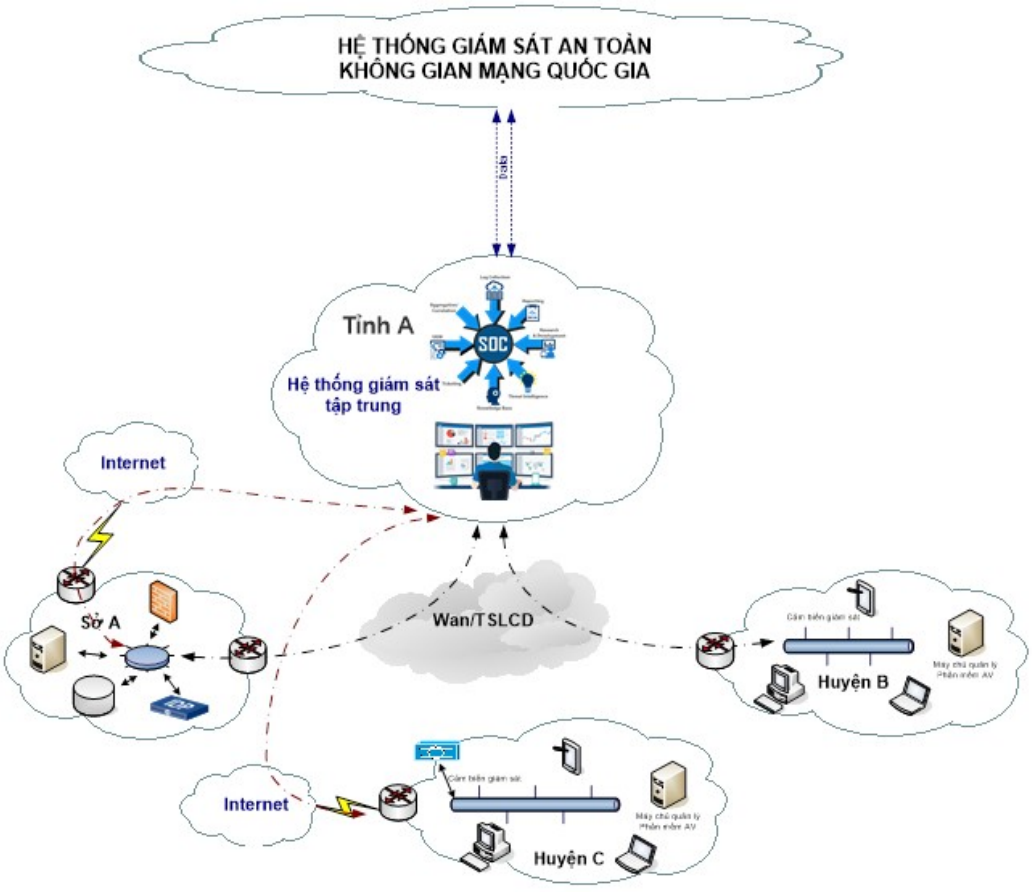
- Hệ thống thông tin có các máy chủ ứng dụng cần được triển khai tập trung tại Trung tâm dữ liệu của bộ, ngành hoặc tỉnh để được giám sát, bảo vệ tập trung.

- Mỗi bộ, ngành, địa phương triển khai một Trung tâm giám sát, điều hành an toàn, an ninh mạng (SOC) theo chỉ đạo của Thủ tướng Chính phủ tại Quyết định 942/QĐ-TTg ngày 15/6/2021. Hệ thống SOC được thiết lập cho phép đơn vị chủ quản có thể nhìn được tổng thể các nguy cơ tấn công mạng đối với các hệ thống thông tin trên địa bàn, thậm chí đến từng máy tính cụ thể bên trong mỗi hệ thống. Theo phương án này, log từ các hệ thống thông tin sẽ được gửi về và được quản lý tại hệ thống quản lý tập trung tại hệ thống SOC.

Hướng dẫn chi tiết việc thiết lập và quản lý vận hành hệ thống giám sát bao gồm các nội dung: (1) Xác định đối tượng và phạm vi giám sát; (2) Hệ thống quản lý tập trung (3) Thiết lập hệ thống giám sát; (4) Quản lý, vận hành hệ thống giám sát được hướng dẫn chi tiết tại ***Phụ lục 8*** tài liệu hướng dẫn này.

4.3.2. Mô hình triển khai giám sát bảo vệ cấp bộ, tỉnh

Theo hướng dẫn tại Mục II, mỗi bộ, tỉnh có nhiều hệ thống thông tin nhằm phân tán tại các đơn vị khác nhau như các cục, vụ, sở, quận, huyện…Nếu đầu tư hệ thống giám sát và bố trí nguồn lực để quản lý vận hành cho mỗi hệ thống này sẽ rất tốn kém và không hiệu quả do tính phân tán, không đồng bộ.



Hình 1. Mô hình tham khảo giám sát tập trung của tỉnh A

Việc triển khai hệ thống giám sát tập trung cho phép đơn vị vận hành có thể nhìn được tổng thể các nguy cơ tấn công mạng đối với các hệ thống thông tin trên địa bàn, thậm chí đến từng máy tính cụ thể bên trong mỗi hệ thống. Việc này sẽ giảm thiểu được chi phí đầu tư và tận dụng và tập trung được nguồn nhân lực có trình độ cao tập trung tại các hệ thống trung tâm.

Do đó, mỗi tỉnh có thể triển khai một hệ thống giám sát tập trung để giám sát và bảo vệ các hệ thống thông tin trên địa bàn. Theo phương án này, log từ

các hệ thống thông tin sẽ được gửi về và được quản lý tại hệ thống quản lý tập trung. Hệ thống quản lý tập trung thường đặt tại trung tâm dữ liệu của tỉnh và do Sở Thông tin và Truyền thông quản lý vận hành.

Các hệ thống thông tin trên địa bàn có hai loại hình triển khai phổ biến:

a) Hệ thống cung cấp dịch vụ trực tuyến và có người sử dụng. Hệ thống này có hệ thống máy chủ để cung cấp dịch vụ và bao gồm cả mạng LAN của người sử dụng (Sở A).

Thông thường các hệ thống này đã được triển khai các hệ thống quan trắc cơ sở, có thể có hệ thống giám sát tập trung và có kết nối mạng Internet độc lập. Đối với trường hợp này, log của hệ thống quan trắc cơ sở sẽ được gửi về hệ thống giám sát tập trung theo một trong hai phương án sau:

- Trường hợp Sở A có kết nối mạng WAN về hệ thống giám sát tập trung thì log sẽ được ưu tiên gửi qua kết nối mạng này. Kết nối WAN cần ưu tiên sử dụng mạng truyền số liệu chuyên dùng (TSLCD).

- Trường hợp Sở A không có kết nối WAN thì log sẽ được gửi qua mạng Internet về hệ thống giám sát tập trung.

Để có phương án tối ưu trong việc gửi log về hệ thống giám sát tập trung, log cần được gửi tập trung về một hệ thống tại Sở A (sử dụng Syslog hoặc giải pháp tương đương) được lọc lấy thông tin cần thiết, nén và mã hóa trước khi gửi về hệ thống tập trung.

Trường hợp hệ thống của Sở A chưa có hệ thống quan trắc thì hệ thống này cần thiết lập tối thiểu cảm biến giám sát và hệ thống quản lý phần mềm phòng chống phần mềm độc hại tập trung và gửi log về hệ thống giám sát trung tâm. Cảm biến giám sát cần được thiết lập để có thể giám sát được cả hai kết nối mạng Internet và WAN.

b) Trường hợp hệ thống chỉ có mạng LAN của người sử dụng. Trường hợp này, hệ thống chỉ có máy tính của người sử dụng và có kết nối mạng Internet.

Kết nối mạng Internet có thể triển khai theo một trong hai phương án sau:

- Hệ thống có kết nối Internet độc lập và không có kết nối WAN (Huyện C). Trường hợp này log của hệ thống quan trắc cơ sở (nếu có) hoặc từ cảm biến giám sát sẽ được gửi về hệ thống giám sát tập trung qua mạng Internet. Chú ý rằng, trường hợp hệ thống có kết nối WAN thì cần ưu tiên sử dụng kết nối này để gửi log về hệ thống giám sát tập trung.

- Hệ thống không có kết nối Internet trực tiếp mà kết nối qua mạng WAN (Huyện B). Trường hợp này, cảm biến giám sát không cần thiết phải triển khai tại Huyện B mà có thể triển khai cảm biến giám sát tập trung tại cổng ra Internet tập trung của các đơn vị. Trường hợp này yêu cầu hệ thống tại các đơn vị không

cấu hình NAT trên các thiết bị mạng để cho phép tại điểm giám sát, cảm biến giám sát có thể thấy được địa chỉ IP thật của mỗi máy tính trong mạng. Việc cấu hình NAT sẽ được thực hiện tại thiết bị định tuyến biên của cổng kết nối Internet tập trung.

Các máy tính trong hệ thống thông tin của Huyện B cần cài đặt phần mềm phòng, chống phần mềm độc hại và được quản lý tập trung bởi một máy tính/máy chủ bên trong hệ thống và gửi log về hệ thống giám sát tập trung.

Các hệ thống thông tin trên địa bàn tỉnh A cần ưu tiên phương án sử dụng kết nối mạng Internet qua kết nối WAN qua cổng kết nối Internet tập trung để có thể triển khai biện pháp giám sát và bảo vệ tập trung nhằm giảm thiểu chi phí đầu tư và tăng hiệu quả giám sát và bảo vệ.

Mỗi hệ thống sử dụng giải pháp phòng, chống phần mềm độc hại có chức năng quản lý tập trung và có thể kết nối, chia sẻ thông tin với hệ thống giám sát an toàn không gian mạng quốc gia.

4.3.3. Hướng dẫn giám sát bảo vệ đối với hệ thống thông tin cấp độ 1

Triển khai đầy đủ biện pháp bảo đảm an toàn thông tin yêu cầu đối với hệ thống thông tin cấp độ 1 theo quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT và theo hướng dẫn dưới đây:

a) Lớp Mạng

Thiết lập cấu hình hệ thống để chia sẻ thông tin kết nối mạng (nếu thiết bị hệ thống hỗ trợ chức năng chia sẻ nhật ký hệ thống) bao gồm các thông tin: Địa chỉ IP nguồn, IP đích; Port nguồn, Port đích về hệ thống SOC.

b) Lớp Máy chủ

- Chia sẻ thông tin về mã độc phát hiện trong hệ thống (nếu phần mềm phòng, chống mã độc hỗ trợ chức năng quản lý tập trung) về hệ thống SOC.

- Thiết lập cấu hình Hệ điều hành của máy chủ cung cấp dịch vụ (nếu hệ điều hành hỗ trợ chức năng chia sẻ nhật ký hệ thống) để chia sẻ nhật ký hệ thống về hệ thống SOC.

c) Lớp Ứng dụng

Thiết lập cấu hình Ứng dụng của máy chủ cung cấp dịch vụ (nếu có) và chia sẻ nhật ký hệ thống về hệ thống SOC.

d) Lớp Thiết bị đầu cuối

Thiết lập cấu hình hệ thống để chia sẻ nhật ký hệ thống của thiết bị đầu cuối (nếu thiết bị đầu cuối hỗ trợ chức năng chia sẻ nhật ký hệ thống) về hệ thống SOC.

4.3.4. Hướng dẫn giám sát bảo vệ đối với hệ thống thông tin cấp độ 2

Triển khai đầy đủ biện pháp bảo đảm an toàn thông tin yêu cầu đối với hệ thống thông tin cấp độ 2 theo quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT và theo hướng dẫn dưới đây:

a) Lớp Mạng

Thiết lập cấu hình hệ thống để chia sẻ nhật ký hệ thống liên quan đến quản lý truy cập và phòng, chống xâm nhập (nếu thiết bị hệ thống hỗ trợ chức năng chia sẻ nhật ký hệ thống) về hệ thống SOC.

b) Lớp Máy chủ

- Chia sẻ thông tin về mã độc phát hiện trong hệ thống (nếu phần mềm phòng, chống mã độc hỗ trợ chức năng quản lý tập trung) về hệ thống SOC;
- Khuyến nghị cài đặt phần mềm Phát hiện và phản ứng sự cố an toàn thông tin trên thiết bị đầu cuối cho các máy chủ cung cấp dịch vụ và kết nối, chia sẻ, quản lý tập trung tại hệ thống SOC;
- Thiết lập cấu hình Hệ điều hành máy chủ (nếu hệ điều hành hỗ trợ chức năng chia sẻ nhật ký hệ thống) để chia sẻ nhật ký hệ thống về hệ thống SOC.

c) Lớp Ứng dụng

- Thiết lập cấu hình Ứng dụng của máy chủ cung cấp dịch vụ (nếu có) và chia sẻ nhật ký hệ thống về hệ thống SOC;
- Cấu hình tường lửa ứng dụng web (nếu có) để chia sẻ nhật ký hệ thống về hệ thống SOC.

c) Lớp Thiết bị đầu cuối

Thiết lập cấu hình hệ thống để chia sẻ nhật ký hệ thống của thiết bị đầu cuối (nếu thiết bị đầu cuối hỗ trợ chức năng chia sẻ nhật ký hệ thống) về hệ thống SOC.

4.3.5. Hướng dẫn giám sát bảo vệ đối với hệ thống thông tin cấp độ 3

Triển khai đầy đủ biện pháp bảo đảm an toàn thông tin yêu cầu đối với hệ thống thông tin cấp độ 3 theo quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT và theo hướng dẫn dưới đây:

a) Lớp Mạng

- Thiết lập cấu hình hệ thống để chia sẻ nhật ký hệ thống về hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung. Nhật ký hệ thống chia sẻ bao gồm các yêu cầu: (1) Đáp ứng yêu cầu tại Mục 7.2.1.4 TCVN 11930:2017; (2) Nhật ký hệ thống phòng chống xâm nhập; (3) Nhật ký hệ thống phòng chống mã độc trên môi trường mạng; (4) Phòng, chống xâm nhập và phòng chống mã độc trên môi trường mạng;

- Chia sẻ nhật ký hệ thống của hệ thống Phòng, chống tấn công từ chối dịch vụ (nếu có) về hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung;

- Thiết lập cấu hình hệ thống của sản phẩm Giám sát hệ thống thông tin tập trung (nếu có) để quản lý tập trung toàn bộ thiết bị mạng, thiết bị bảo mật, máy chủ, ứng dụng; Chia sẻ nhật ký của sản phẩm Giám sát hệ thống thông tin tập trung về hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung.

- Thiết lập cấu hình hệ thống của hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung để quản lý tập trung nhật ký hệ thống của toàn bộ thiết bị mạng, thiết bị bảo mật, máy chủ, ứng dụng;

- Chia sẻ nhật ký hệ thống của sản phẩm Quản lý và phân tích sự kiện an toàn thông tin tập trung về hệ thống SOC; Trường hợp hệ thống SOC được triển khai trên hạ tầng dùng chung của Trung tâm dữ liệu thì hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung là một hợp phần của hệ thống SOC.

b) Lớp Máy chủ

- Chia sẻ thông tin về mã độc phát hiện trong hệ thống về hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung;

- Chia sẻ nhật ký hệ thống của hệ thống Phát hiện và phản ứng sự cố an toàn thông tin trên thiết bị đầu cuối (nếu có) về hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung;

- Thiết lập cấu hình Hệ điều hành của máy chủ cung cấp dịch vụ (nếu có) để chia sẻ nhật ký hệ thống về hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung. Nhật ký hệ thống chia sẻ đáp ứng yêu cầu tại Mục 7.2.2.3 TCVN 11930:2017.

c) Lớp Ứng dụng

- Cấu hình tường lửa ứng dụng web (nếu có) để chia sẻ nhật ký hệ thống về hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung;

- Thiết lập cấu hình Ứng dụng của máy chủ cung cấp dịch vụ (nếu có) và chia sẻ nhật ký hệ thống về hệ thống Quản lý và phân tích sự kiện an toàn thông

tin tập trung. Nhật ký hệ thống chia sẻ đáp ứng yêu cầu tại Mục 7.2.3.3 TCVN 11930:2017;

- Chia sẻ nhật ký hệ thống của hệ thống Tường lửa cơ sở dữ liệu (nếu có) về hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung;

- Chia sẻ nhật ký hệ thống của hệ thống bảo đảm an toàn thông tin cho hệ thống thư điện tử (nếu có) về hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung;

- Chia sẻ nhật ký hệ thống của hệ thống Phòng, chống thất thoát dữ liệu (nếu có) về hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung.

d) Lớp Thiết bị đầu cuối

- Chia sẻ nhật ký hệ thống của hệ thống Quản lý truy cập lớp mạng (nếu có) về hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung.

- Thiết lập cấu hình hệ thống để chia sẻ nhật ký hệ thống của thiết bị đầu cuối (nếu thiết bị đầu cuối hỗ trợ chức năng chia sẻ nhật ký hệ thống) về hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung.

4.3.6. Hướng dẫn giám sát bảo vệ đối với hệ thống thông tin cấp độ 4

Triển khai đầy đủ biện pháp bảo đảm an toàn thông tin yêu cầu đối với hệ thống thông tin cấp độ 4 theo quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT và theo hướng dẫn dưới đây:

a) Lớp Mạng

- Thiết lập cấu hình hệ thống để chia sẻ nhật ký hệ thống về hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung. Nhật ký hệ thống chia sẻ bao gồm các yêu cầu: (1) Đáp ứng yêu cầu tại Mục 8.2.1.4 TCVN 11930:2017; (2) Nhật ký hệ thống phòng chống xâm nhập; (3) Nhật ký hệ thống phòng chống mã độc trên môi trường mạng; (4) Phòng, chống xâm nhập và phòng chống mã độc trên môi trường mạng;

- Chia sẻ nhật ký hệ thống của hệ thống Phòng, chống tấn công từ chối dịch vụ (nếu có) về hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung;

- Chia sẻ nhật ký hệ thống của hệ thống Phòng, chống tấn công từ chối dịch vụ (nếu có) về hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung;

- Chia sẻ nhật ký hệ thống của hệ thống Quản lý tài khoản đặc quyền (nếu có) về hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung;

- Thiết lập cấu hình hệ thống của sản phẩm Giám sát hệ thống thông tin tập trung (nếu có) để quản lý tập trung toàn bộ thiết bị mạng, thiết bị bảo mật, máy chủ, ứng dụng; Chia sẻ nhật ký của sản phẩm Giám sát hệ thống thông tin tập trung về hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung.

- Thiết lập cấu hình hệ thống của hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung để quản lý tập trung nhật ký hệ thống của toàn bộ thiết bị mạng, thiết bị bảo mật, máy chủ, ứng dụng;

- Chia sẻ nhật ký hệ thống của sản phẩm Quản lý và phân tích sự kiện an toàn thông tin tập trung về hệ thống SOC; Trường hợp hệ thống SOC được triển khai trên hạ tầng dùng chung của Trung tâm dữ liệu thì hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung là một hợp phần của hệ thống SOC.

b) Lớp Máy chủ

- Chia sẻ thông tin về mã độc phát hiện trong hệ thống về hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung;

- Chia sẻ nhật ký hệ thống của hệ thống Phát hiện và phản ứng sự cố an toàn thông tin trên thiết bị đầu cuối (nếu có) vệ hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung;

- Thiết lập cấu hình Hệ điều hành của máy chủ cung cấp dịch vụ (nếu có) để chia sẻ nhật ký hệ thống về hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung. Nhật ký hệ thống chia sẻ đáp ứng yêu cầu tại Mục 8.2.2.3 TCVN 11930:2017.

c) Lớp Ứng dụng

- Cấu hình tường lửa ứng dụng web (nếu có) để chia sẻ nhật ký hệ thống về hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung;

- Thiết lập cấu hình Ứng dụng của máy chủ cung cấp dịch vụ (nếu có) và chia sẻ nhật ký hệ thống về hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung. Nhật ký hệ thống chia sẻ đáp ứng yêu cầu tại Mục 8.2.3.3 TCVN 11930:2017;

- Chia sẻ nhật ký hệ thống của hệ thống Tường lửa cơ sở dữ liệu (nếu có) về hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung;

- Chia sẻ nhật ký hệ thống của hệ thống bảo đảm an toàn thông tin cho hệ thống thư điện tử (nếu có) về hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung;

- Chia sẻ nhật ký hệ thống của hệ thống Phòng, chống thất thoát dữ liệu (nếu có) về hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung.

d) Lớp Thiết bị đầu cuối

- Chia sẻ nhật ký hệ thống của hệ thống Quản lý truy cập lớp mạng (nếu có) về hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung.

- Thiết lập cấu hình hệ thống để chia sẻ nhật ký hệ thống của thiết bị đầu cuối (nếu thiết bị đầu cuối hỗ trợ chức năng chia sẻ nhật ký hệ thống) về hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung.

4.3.7. Hướng dẫn giám sát bảo vệ đối với hệ thống thông tin cấp độ 5

Triển khai đầy đủ biện pháp bảo đảm an toàn thông tin yêu cầu đối với hệ thống thông tin cấp độ 5 theo quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT và theo hướng dẫn dưới đây:

a) Lớp Mạng

- Thiết lập cấu hình hệ thống để chia sẻ nhật ký hệ thống về hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung. Nhật ký hệ thống chia sẻ bao gồm các yêu cầu: (1) Đáp ứng yêu cầu tại Mục 9.2.1.4 TCVN 11930:2017; (2) Nhật ký hệ thống phòng chống xâm nhập; (3) Nhật ký hệ thống phòng chống mã độc trên môi trường mạng; (4) Phòng, chống xâm nhập và phòng chống mã độc trên môi trường mạng;

- Chia sẻ nhật ký hệ thống của hệ thống Phòng, chống tấn công từ chối dịch vụ (nếu có) về hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung;

- Chia sẻ nhật ký hệ thống của hệ thống Phòng, chống tấn công từ chối dịch vụ (nếu có) về hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung;

- Chia sẻ nhật ký hệ thống của hệ thống Quản lý tài khoản đặc quyền (nếu có) về hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung;

- Thiết lập cấu hình hệ thống của sản phẩm Giám sát hệ thống thông tin tập trung (nếu có) để quản lý tập trung toàn bộ thiết bị mạng, thiết bị bảo mật, máy chủ, ứng dụng; Chia sẻ nhật ký của sản phẩm Giám sát hệ thống thông tin tập trung về hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung;

- Thiết lập cấu hình hệ thống của hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung để quản lý tập trung nhật ký hệ thống của toàn bộ thiết bị mạng, thiết bị bảo mật, máy chủ, ứng dụng;

- Chia sẻ nhật ký hệ thống của sản phẩm Quản lý và phân tích sự kiện an toàn thông tin tập trung về hệ thống SOC; Trường hợp hệ thống SOC được triển khai trên hạ tầng dùng chung của Trung tâm dữ liệu thì hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung là một hợp phần của hệ thống SOC.

b) Lớp Máy chủ

- Chia sẻ thông tin về mã độc phát hiện trong hệ thống về hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung;

- Chia sẻ nhật ký hệ thống của hệ thống Phát hiện và phản ứng sự cố an toàn thông tin trên thiết bị đầu cuối (nếu có) vệ hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung;

- Thiết lập cấu hình Hệ điều hành của máy chủ cung cấp dịch vụ (nếu có) để chia sẻ nhật ký hệ thống về hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung. Nhật ký hệ thống chia sẻ đáp ứng yêu cầu tại Mục 9.2.2.3 TCVN 11930:2017.

c) Lớp Ứng dụng

- Cấu hình tường lửa ứng dụng web (nếu có) để chia sẻ nhật ký hệ thống về hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung;

- Thiết lập cấu hình Ứng dụng của máy chủ cung cấp dịch vụ (nếu có) và chia sẻ nhật ký hệ thống về hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung. Nhật ký hệ thống chia sẻ đáp ứng yêu cầu tại Mục 9.2.3.3 TCVN 11930:2017;

- Chia sẻ nhật ký hệ thống của hệ thống Tường lửa cơ sở dữ liệu (nếu có) về hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung;

- Chia sẻ nhật ký hệ thống của hệ thống bảo đảm an toàn thông tin cho hệ thống thư điện tử (nếu có) về hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung;

- Chia sẻ nhật ký hệ thống của hệ thống Phòng, chống thất thoát dữ liệu (nếu có) về hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung.

d) Lớp Thiết bị đầu cuối

- Chia sẻ nhật ký hệ thống của hệ thống Quản lý truy cập lớp mạng (nếu có) về hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung.

- Thiết lập cấu hình hệ thống để chia sẻ nhật ký hệ thống của thiết bị đầu cuối (nếu thiết bị đầu cuối hỗ trợ chức năng chia sẻ nhật ký hệ thống) về hệ thống Quản lý và phân tích sự kiện an toàn thông tin tập trung.

4.3.8. Hướng dẫn triển khai Trung tâm điều hành an toàn mạng SOC

a) Hướng dẫn triển khai hệ thống SOC

Như đã được hướng dẫn ở trên, mỗi bộ, ngành, địa phương triển khai một Trung tâm SOC theo chỉ đạo của Thủ tướng Chính phủ tại Quyết định 942/QĐ-TTg ngày 15/6/2021. Hệ thống SOC được thiết lập để giám sát, bảo vệ tập trung các hệ thống thông tin thuộc phạm vi quản lý của mỗi bộ, ngành, địa phương.

Các hệ thống thuộc phạm vi quản lý của bộ, ngành, địa phương yêu cầu triển khai đầy đủ các biện phạm bảo vệ theo quy định tại Điều 9, Điều 10 Thông

tư 12/2022/TT-BTTTT và thiết lập cấu hình hệ thống để kết nối, chia sẻ dữ liệu về hệ thống SOC để giám sát, bảo vệ tập trung mà không cần thiết lập hệ thống SOC cho riêng hệ thống của mình.

Hệ thống SOC thuộc loại hình hệ thống cơ sở hạ tầng thông tin. Hệ thống SOC khi triển khai giám sát, bảo vệ tập trung cho các hệ thống thông tin thuộc bộ, ngành, địa phương có cấp độ an toàn thông tin tối thiểu cấp độ 3. Do đó, hệ thống SOC phải triển khai đầy đủ các biện phạm bảo vệ theo quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT và bổ sung các thành phần để giám sát, bảo vệ tập trung các hệ thống thông tin khác.

Hệ thống SOC có thể được triển khai theo một số phương án tùy thuộc vào hiện trạng hiện có của mỗi bộ, ngành, địa phương như sau:

Trường hợp, bộ, ngành, địa phương đã có Trung tâm dữ liệu (TTDL) thì hệ thống SOC nên được triển khai trên hệ thống TTDL và coi như một hệ thống hợp phần của TTDL và bổ sung các phương án giám sát, bảo vệ để đáp ứng các yêu cầu kỹ thuật được hướng dẫn tại văn bản này. Tuy nhiên, khi triển khai theo phương án này thì yêu cầu đơn vị vận hành phải có đủ năng lực để vận hành, khai thác hiệu quả của hệ thống SOC.

Trong trường hợp cơ quan, tổ chức chưa triển khai TTDL hoặc đơn vị vận hành không đủ năng lực vận hành, khai thác hiệu quả hệ thống SOC thì có thể xem xét phương án triển khai SOC theo hình thức thuê dịch vụ. Trong trường hợp này, bên cung cấp dịch vụ sẽ cung cấp hạ tầng và giải pháp. Bên sử dụng chỉ đầu tư các thành phần đầu cuối cơ bản như màn hình, máy tính quản trị và cơ sở hạ tầng liên quan để phục vụ việc thực hiện quản lý, vận hành SOC từ xa.

Yêu cầu về năng lực đối với bên cung cấp dịch vụ SOC cơ quan, tổ chức có thể kham khảo tại tại Quyết định 1356/QĐ-BTTTT ngày 07/7/2022 Ban hành Tiêu chí đánh giá giải pháp, dịch vụ Trung tâm giám sát điều hành an toàn, an ninh mạng (SOC).

Mô hình triển khai được hướng dẫn tại Mục 4.3.2 hướng dẫn này.

Cơ quan, tổ chức cần ưu tiên lựa chọn giải pháp do doanh nghiệp Việt Nam làm chủ về công nghệ, sử dụng dịch vụ của các doanh nghiệp trong nước đáp ứng các yêu cầu kỹ thuật theo quy định, theo chỉ đạo của Thủ tướng Chính phủ tại điểm đ, Khoản 1 Chỉ thị số 14/CT-TTg ngày 07/6/2019.

b) Yêu cầu đối với hệ thống SOC

i. Yêu cầu về bảo đảm an toàn hệ thống thông tin theo cấp độ

- Hệ thống SOC được xác định cấp độ, xây dựng, thẩm định và phê duyệt Hồ sơ đề xuất cấp độ theo quy định;

- Hệ thống SOC được triển khai đầy đủ phương án bảo vệ theo quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT.

ii. Yêu cầu đối với thành phần giám sát, bảo vệ của hệ thống SOC

Các giải pháp sử dụng trong hệ thống SOC được khuyến nghị sử dụng các giải pháp đáp ứng các yêu cầu kỹ thuật đối với sản phẩm tương ứng do Bộ Thông tin và Truyền thông ban hành.

iii. Có sản phẩm Quản lý và phân tích sự kiện an toàn thông tin – SIEM, đáp ứng các yêu cầu sau:

Giải pháp SIEM triển khai phải bảo đảm năng lực thu thập và quản lý nhật ký hệ thống của toàn bộ các nguồn log gửi về từ các hệ thống thông tin trên địa bàn hoặc thuộc phạm vi quản lý.

Nhật ký hệ thống bao gồm đầy đủ log của thiết bị mạng, thiết bị bảo mật. máy chủ, ứng dụng của hệ thống SOC và các hệ thống được giám sát, bảo vệ bởi hệ thống SOC;

iv. Có sản phẩm Phòng, chống xâm nhập lớp mạng – NIPS, đáp ứng các yêu cầu sau:

Giải pháp NIPS được triển khai tại hệ thống SOC để bảo vệ hệ thống SOC theo các quy định về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Đối với các hệ thống thuộc phạm vi giám sát, bảo vệ của hệ thống SOC thì triển khai hệ thống NIPS cho các hệ thống thông tin phục vụ người dân, doanh nghiệp và cơ quan, tổ chức nhà nước, hệ thống thông tin cấp huyện, cấp sở hoặc hệ thống mạng LAN có quy mô từ 150 người sử dụng trở lên;

v. Có sản phẩm Phòng, chống mã độc – AV, đáp ứng các yêu cầu sau:

Giải pháp AV quản lý tập trung được toàn bộ máy chủ, máy trạm phục vụ hoạt động của hệ thống SOC và từ các hệ thống thuộc phạm vi bảo vệ của hệ thống SOC;

Giải pháp AV có chức năng kết nối, chia sẻ thông tin về Trung tâm Giám sát an toàn thông tin mạng quốc gia.

vi. Có sản phẩm Phát hiện và phản ứng sự cố an toàn thông tin trên thiết bị đầu cuối – EDR, đáp ứng các yêu cầu sau:

Giải pháp EDR quản lý tập trung được toàn bộ máy chủ, máy trạm phục vụ hoạt động của hệ thống SOC và từ các hệ thống thuộc phạm vi bảo vệ của hệ thống SOC;

Giải pháp EDR có chức năng kết nối, chia sẻ thông tin về Trung tâm Giám sát an toàn thông tin mạng quốc gia.

vii. Có sản phẩm Tường lửa ứng dụng web – WAF, đáp ứng các yêu cầu sau:

Giải pháp WAF giám sát, bảo vệ tập trung được toàn bộ các cổng/trang thông tin điện tử thuộc phạm vi giám sát, bảo vệ của SOC;

- Có sản phẩm Điều phối, tự động hóa và phản ứng an toàn thông tin – SOAR hoặc sản phẩm có chức năng tích hợp tương đương.

- Có sản phẩm Nền tảng tri thức mối đe dọa an toàn thông tin – TIP hoặc sản phẩm có chức năng tích hợp tương đương.

- Có sản phẩm Quản lý điểm yếu an toàn thông tin tập trung hoặc sản phẩm có chức năng tích hợp tương đương.

4.4. Kiểm tra, đánh giá an toàn thông tin - Lớp 3

4.4.1. Hướng dẫn chung

Cơ quan, tổ chức thực hiện kiểm tra, đánh giá an toàn thông tin theo quy định tại Điều 11, 12 Thông tư số 12/2022/TT-BTTTT và hướng dẫn cụ thể dưới đây.

Chủ quản hệ thống thông tin chỉ đạo đơn vị chuyên trách về an toàn thông tin chủ trì tổ chức, kiểm tra đánh giá, tổng hợp và xây dựng báo cáo việc tuân thủ các quy định của pháp luật về bảo đảm an toàn hệ thống thông tin mạng theo trách nhiệm của chủ quản hệ thống thông tin;

Đơn vị chuyên trách về an toàn thông tin tổ chức kiểm tra, đánh giá việc tuân thủ các quy định của pháp luật về bảo đảm an toàn hệ thống thông tin mạng đối với các đơn vị vận hành trên địa bàn; tổng hợp và chuẩn bị nội dung báo cáo đánh giá tuân thủ cho chủ quản hệ thống thông tin;

Đơn vị vận hành tự thực hiện kiểm tra, đánh giá hoặc thuê dịch vụ chuyên nghiệp của doanh nghiệp thực hiện. Đối với hệ thống từ cấp độ 3 trở lên phải do tổ chức chuyên môn được cơ quan có thẩm quyền cấp phép; tổ chức sự nghiệp nhà nước có chức năng, nhiệm vụ phù hợp hoặc do tổ chức chuyên môn được cấp có thẩm quyền chỉ định thực hiện). Đơn vị cung cấp dịch vụ được cấp Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng có thể tư vấn xây dựng Hồ sơ đánh giá tuân thủ và/hoặc xác nhận kết quả kiểm tra, đánh giá theo yêu cầu của bên sử dụng dịch vụ. Đối với công tác kiểm tra, đánh giá an toàn thông tin mạng cho hệ thống thông tin thuộc quyền quản lý cần lựa chọn tổ chức, doanh nghiệp độc lập với tổ chức, doanh nghiệp giám sát, bảo vệ để định kỳ kiểm tra, đánh giá an toàn thông tin mạng đối với hệ thống thông tin cấp độ 3 trở lên thuộc quyền quản lý hoặc kiểm tra, đánh giá đột xuất khi có yêu cầu theo quy định của pháp luật.

Hồ sơ đánh giá tuân thủ các quy định của pháp luật về bảo đảm an toàn hệ thống thông tin bao gồm: (1) Quyết định phê duyệt Hồ sơ đề xuất cấp độ và Quy chế bảo đảm an toàn thông tin; (2) Báo cáo kết quả kiểm tra, đánh giá hiệu quả của các biện pháp bảo đảm an toàn thông tin theo phương án bảo đảm an toàn thông tin được phê duyệt; (3) Báo cáo kết quả kiểm tra, đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống thông tin.

4.4.2. Hướng dẫn thực hiện kiểm tra, đánh giá hiệu quả của các biện pháp bảo đảm an toàn thông tin

Đánh giá hiệu quả của các biện pháp bảo đảm an toàn thông tin bao gồm các nội dung và được hướng dẫn cụ thể như dưới đây.

a) Kiểm tra tính đầy đủ và phù hợp của Quy chế bảo đảm an toàn thông tin theo phương án bảo đảm an toàn thông tin về quản lý trong Hồ sơ đề xuất cấp độ được phê duyệt

Quy chế bảo đảm an toàn thông tin được đánh giá là phù hợp khi nội dung Quy chế bao gồm đầy đủ các quy định và quy trình đáp ứng các yêu cầu về quản lý được quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT và Tiêu chuẩn quốc gia TCVN 11930-2017, bao gồm:

- Các quy định trong Quy chế: (1) Thiết lập chính sách an toàn thông tin; (2) Tổ chức bảo đảm an toàn thông tin; (3) Bảo đảm nguồn nhân lực; (4) Quản lý thiết kế, xây dựng hệ thống; (5) Quản lý vận hành hệ thống;

- Các quy trình kèm theo Quy chế: (1) Quy trình tuyển dụng cán bộ; (2) Quy trình chấm dứt hoặc thay đổi công việc; (3) Quy trình thử nghiệm và nghiệm thu hệ thống; (4) Quản lý an toàn mạng; (5) Quản lý an toàn máy chủ và ứng dụng; (6) Quản lý an toàn dữ liệu; (7) Quản lý an toàn thiết bị đầu cuối; (8) Quản lý phòng chống phần mềm độc hại; (9) Quản lý giám sát an toàn hệ thống thông tin; (10) Quản lý điểm yếu an toàn thông tin; (11) Quản lý sự cố an toàn thông tin; (12) Quản lý an toàn người sử dụng đầu cuối; (13) Quản lý rủi ro an toàn thông tin; (14) Kết thúc vận hành, khai thác, thanh lý, hủy bỏ.

b) Đánh giá việc tuân thủ các quy định, quy trình trong Quy chế bảo đảm an toàn thông tin trong quá trình vận hành, khai thác, kết thúc hoặc hủy bỏ hệ thống thông tin

- Đơn vị vận hành cần có nhật ký quản lý vận hành hệ thống theo các quy định và quy trình ban hành theo Quy chế bảo đảm an toàn thông tin.

- Báo cáo đánh giá tuân thủ cần có các tài liệu minh chứng hệ thống được quản lý, vận hành theo Quy chế được ban hành là nhật ký vận hành hệ thống.

c) Đánh giá việc thiết kế hệ thống theo phương án được phê duyệt trong Hồ sơ đề xuất cấp độ:

Báo cáo đánh giá tuân thủ cần có sơ đồ vật lý, sơ đồ logic và minh chứng cấu hình trên thiết bị hệ thống để chứng minh hệ thống được thiết kế đúng theo phương án được phê duyệt trong Hồ sơ đề xuất cấp độ.

d) Đánh giá việc thiết lập, cấu hình hệ thống theo phương án trong Hồ sơ đề xuất cấp độ được phê duyệt

Mỗi thành phần trong hệ thống như thiết bị hệ thống, máy chủ, ứng dụng được đưa ra tại các Danh mục trong Hồ sơ đề xuất cấp độ cần có một báo cáo minh chứng việc thiết lập, cấu hình hệ thống theo phương án trong Hồ sơ đề xuất cấp độ được phê duyệt.

4.4.3. Hướng dẫn kiểm tra, đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống thông tin

Kiểm tra, đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống thông tin bao gồm các nội dung và được hướng dẫn cụ thể như dưới đây.

a) Phạm vi, đối tượng đánh giá

Toàn bộ thành phần trong hệ thống như thiết bị hệ thống, máy chủ, ứng dụng được đưa ra tại các Danh mục trong Hồ sơ đề xuất cấp độ.

b) Tiêu chí đánh giá

i. Tiêu chí đánh giá thiết bị hệ thống được chia thành các nhóm sau:

- Thiết bị mạng lớp 2: Đánh giá vai trò thiết bị trong hệ thống; Kiểm tra, đánh giá cấu hình lớp an ninh; Kiểm tra, đánh giá cấu hình quản trị; Kiểm tra, đánh giá cấu hình chung: phiên bản, lỗ hổng của thiết bị; Kiểm tra, đánh giá cấu hình chính sách tài khoản; Kiểm tra chính sách kết nối quản trị; Kiểm tra cấu hình log, giám sát.

- Thiết bị mạng lớp 3: Đánh giá vai trò thiết bị trong hệ thống; Kiểm tra, đánh giá cấu hình lớp an ninh; Kiểm tra, đánh giá cấu hình quản trị; Kiểm tra, đánh giá cấu hình chung: phiên bản, lỗ hổng của thiết bị; Kiểm tra, đánh giá cấu hình chính sách tài khoản; Kiểm tra chính sách kết nối quản trị; Kiểm tra cấu hình log, giám sát; Kiểm tra, đánh giá cấu hình định tuyến (thiết bị mạng).

- Thiết bị bảo mật: Đánh giá vai trò thiết bị trong hệ thống; Kiểm tra, đánh giá cấu hình lớp an ninh; Kiểm tra, đánh giá cấu hình quản trị; Kiểm tra, đánh giá cấu hình chung: phiên bản, lỗ hổng của thiết bị; Kiểm tra, đánh giá cấu hình chính sách tài khoản; Kiểm tra chính sách kết nối quản trị; Kiểm tra cấu hình

log, giám sát; Kiểm tra, đánh giá cấu hình định tuyến; Kiểm tra chính sách, cấu hình ngăn chặn tấn công trên thiết bị.

ii. Tiêu chí đánh giá đối với máy chủ bao gồm nhưng không giới hạn các tiêu chí sau:

- Kiểm tra bản vá và cập nhật hệ điều hành

- Kiểm tra cấu hình hệ điều hành

- Kiểm tra cấu hình chứng thực

- Kiểm tra cấu hình log, giám sát

- Kiểm tra các cấu hình chính sách nội bộ

- Kiểm tra, đánh giá cấu hình chính sách tài khoản

- Kiểm tra chính sách kết nối quản trị

- Kiểm tra các giải pháp về phòng, chống mã độc

- Các tiêu chí khác theo CIS Server Benchmark

iii. Tiêu chí đánh giá đối với ứng dụng bao gồm nhưng không giới hạn các tiêu chí sau:

- Kiểm tra tính an toàn của các thư viện mã nguồn

- Kiểm tra, đánh giá Quản lý cấu hình & triển khai

- Kiểm tra, đánh giá Quản lý định danh

- Kiểm tra, đánh giá Xác thực

- Kiểm tra, đánh giá Phân quyền

- Kiểm tra, đánh giá Quản lý phiên

- Kiểm tra, đánh giá Sàng lọc dữ liệu đầu vào

- Kiểm tra, đánh giá Cơ chế xử lý lỗi

- Kiểm tra, đánh giá Thuật toán mã hóa

- Kiểm tra, đánh giá Logic nghiệp vụ

- Kiểm tra Xử lý phía người dùng

- Kiểm tra, đánh giá khả năng tồn tại các lỗ hổng overflows, SQL Injection, Race Conditions

c) Phương pháp kiểm tra, đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống thông tin

i. Kiểm tra, đánh giá hộp đen (Black box):

Người đánh giá sẽ thực hiện kiểm tra hệ thống từ bên ngoài và không được cung cấp các thông tin về hệ thống mục tiêu như nền tảng hệ thống, phiên bản ứng dụng, sơ đồ kiến trúc, tài khoản đăng nhập.v.v.

ii. Kiểm tra, đánh giá hộp xám (Gray box):

Người đánh giá được cung cấp một số thông tin về hệ thống được đánh giá. Hình thức này có lợi thế cho phép đánh giá được các vùng chức năng đòi hỏi phải đăng nhập mới có thể tiếp cận, kết quả Kiểm tra, đánh giá an toàn thông tin sẽ đầy đủ hơn so với blackbox

iii. Kiểm tra, đánh giá hộp trắng (White box):

Người đánh giá sẽ được cung cấp đầy đủ thông tin và được tiếp cận trực tiếp với về hệ thống, ứng dụng, mã nguồn, cấu hình để thực hiện một đánh giá tổng thể và đầy đủ nhất.

4.5. Kết nối, chia sẻ dữ liệu - Lớp 4

4.5.1. Hướng dẫn chung

Kết nối, chia sẻ dữ liệu giám sát về Trung tâm Giám sát an toàn không gian mạng quốc gia nhằm mục đích hỗ trợ đảm bảo an toàn không gian mạng quốc gia và hỗ trợ cơ quan, tổ chức trong việc giám sát bảo vệ hệ thống thông tin.

Kết nối chia sẻ dữ liệu lớp 4 của cơ quan, tổ chức cần tổ chức, cần bảo đảm bao gồm các dữ liệu sau:

- Chia sẻ dữ liệu giám sát hệ thống giám sát tập trung của các bộ, ngành, địa phương về Trung tâm Giám sát an toàn không gian mạng quốc gia.

- Chia sẻ dữ liệu phòng, chống mã độc tập trung của các bộ, ngành, địa phương về Trung tâm Giám sát an toàn không gian mạng quốc gia.

Kết nối, chia sẻ dữ liệu về Trung tâm Giám sát an toàn không gian mạng quốc gia, đảm bảo các yêu cầu kỹ thuật dưới đây:

- Dữ liệu chia sẻ phải bảo đảm thường xuyên, liên tục. Không mất kết nối quá 01 ngày.

- Dữ liệu chia sẻ phải bảo đảm tính đầy đủ và tuân thủ chuẩn kết nối theo hướng dẫn tại hướng dẫn này.

- Đối với dữ liệu giám sát cần chia sẻ đầy đủ các cảnh báo có mức độ nguy hiểm từ thấp đến nghiêm trọng, yêu cầu đơn vị đảm bảo chia sẻ **đầy đủ 100% các cảnh báo mức cao và nghiêm trọng**.

4.5.2. Hướng dẫn kết nối, chia sẻ dữ liệu giám sát an toàn thông tin về Trung tâm Giám sát an toàn không gian mạng quốc gia

a) Hướng dẫn chung

Việc kết nối, chia sẻ thông tin từ hệ thống của cơ quan, tổ chức với Hệ thống xử lý tấn công mạng Internet Việt Nam (Hệ thống tiếp nhận và xử lý dữ liệu giám sát quốc gia) của Bộ Thông tin và Truyền thông, giúp phát hiện và cảnh báo sớm nguy cơ mất an toàn thông tin có thể xảy ra với cơ quan, tổ chức và phục vụ công tác quản lý nhà nước của Bộ Thông tin và Truyền thông.

Địa chỉ hệ thống kỹ thuật tiếp nhận thông tin:

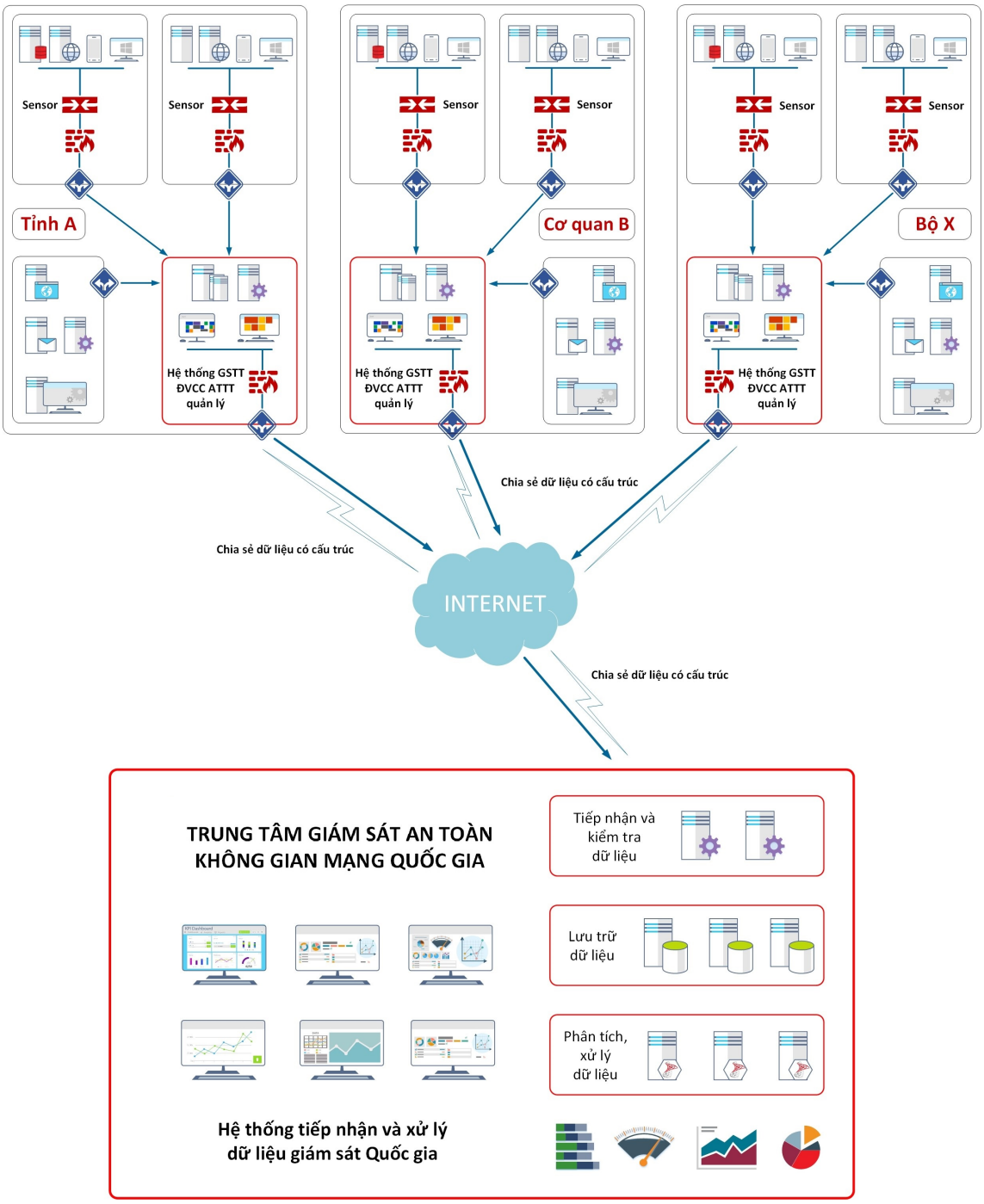
- Địa chỉ trên Internet: https://monitor.soc.gov.vn.

- Địa chỉ trên mạng truyền số liệu chuyên dùng: https://10.21.124.2

Để kết nối chia sẻ thông tin, tổ chức cung cấp thông tin (theo hướng dẫn dưới đây) Cục An toàn thông tin sẽ cấp tài khoản xác thực.

Trong quá trình thực hiện, nếu cần hỗ trợ có thể liên hệ đầu mối kỹ thuật của Cục An toàn thông tin để được hướng dẫn kỹ thuật cụ thể theo thư điện tử: ais@mic.gov.vn; điện thoại: 024.3209.1616.

b) Mô hình triển khai



Hình 2. Mô hình triển khai kết nối, chia sẻ dữ liệu giám sát an toàn thông tin

Như đã hướng dẫn tại Mục 4.3.2, mỗi bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Uỷ ban nhân dân các tỉnh, thành phố trực thuộc Trung ương có tối thiểu 01 hệ thống SOC để giám sát và hỗ trợ bảo vệ tập trung các hệ thống thông tin thuộc phạm vi quản lý của bộ, tỉnh.

Hệ thống SOC tiếp nhận, xử lý và chia sẻ nhật ký hệ thống của các hệ thống thông tin thuộc phạm vi quản lý của bộ tỉnh về Trung tâm Giám sát an toàn không gian mạng quốc gia, Cục An toàn thông tin quản lý và vận hành.

Phương thức kết nối và định dạng thông tin, dữ liệu chia sẻ được hướng dẫn ở dưới đây.

c) Phương thức kết nối

Việc chia sẻ thông tin giữa Hệ thống giám sát trung tâm cấp bộ, ngành, địa phương của các cơ quan đơn vị với Hệ thống tiếp nhận và xử lý dữ liệu giám sát quốc gia của Bộ Thông tin và Truyền thông được truyền đi qua kênh mã hoá HTTPS.

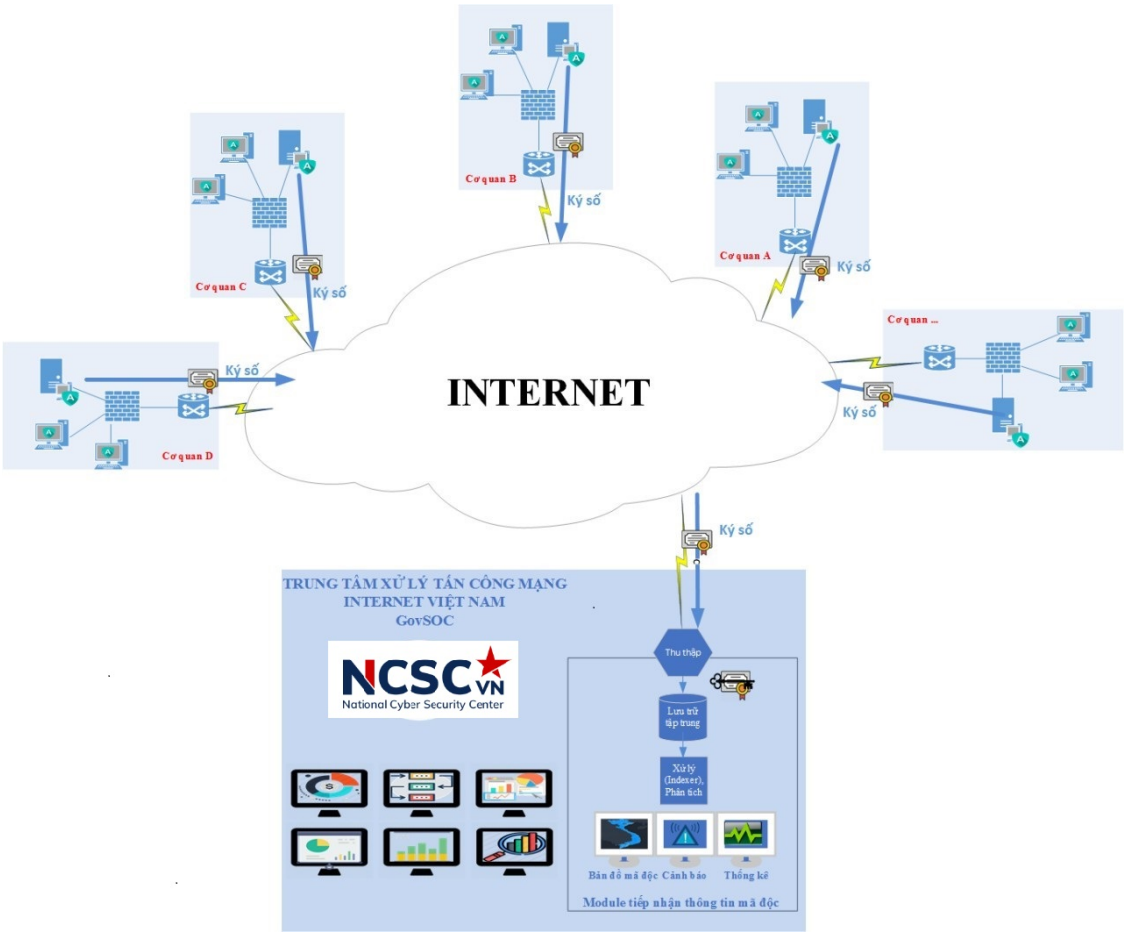
Thông tin chia sẻ bao gồm các trường được mô tả trong Phụ lục 3 và đóng gói theo chuẩn JSON.

d) Định dạng thông tin, dữ liệu chia sẻ

Việc kết nối, chia sẻ thông tin giữa các hệ thống kỹ thuật thực hiện trên cơ sở áp dụng định dạng dữ liệu JSON với các trường dữ liệu theo quy định tại Phụ lục 4 hướng dẫn này. Việc xác định quy cách đóng gói gói tin do doanh nghiệp cung cấp giải pháp quyết định dựa trên cơ sở đáp ứng yêu cầu do cơ quan có nhu cầu khai thác đặt ra.

4.5.2. Hướng dẫn kiểm tra kết nối đối với chia sẻ dữ liệu phòng, chống mã độc tập trung của các bộ, ngành, địa phương về Trung tâm Giám sát an toàn không gian mạng quốc gia

a) Mô hình triển khai



Các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Uỷ ban nhân dân các tỉnh, thành phố trực thuộc Trung ương có giải pháp phòng, chống mã độc được đầu tư mới hoặc nâng cấp cần có chức năng cho phép quản trị tập trung, có thể chia sẻ thông tin, dữ liệu thống kê tình hình lây nhiễm mã độc với hệ thống kỹ thuật của Bộ Thông tin và Truyền thông (Cục An toàn thông tin).

Do vậy mỗi cơ quan tổ chức khi triển khai các giải pháp phòng, chống mã độc cần có máy chủ quản lý tập trung về tình hình lây nhiễm, phòng chống mã độc của các máy tính, thiết bị mạng trong nội bộ cơ quan, tổ chức và chia sẻ thông tin cơ bản với hệ thống kỹ thuật của Bộ Thông tin và Truyền thông.

Việc kết nối, chia sẻ thông tin về mã độc giúp cập nhật tình hình lây nhiễm mã độc chung tại Việt Nam. Các cơ quan tổ chức gửi thông tin về Bộ

Thông tin và Truyền thông (Cục An toàn thông tin) có thể cập nhật tình hình của tổ chức mình và tổ chức khác thông qua bản đồ lây nhiễm mã độc tại Việt Nam.

Với các mẫu, thông tin mã độc thu thập được, thông qua xử lý và chia sẻ lại của Bộ Thông tin và Truyền thông (Cục An toàn thông tin) sẽ hỗ trợ cơ quan tổ chức khác có thể phòng, chống, ngăn chặn nguy cơ tấn công tương tự khi bị đối tượng tấn công sử dụng cùng mẫu mã độc, giúp tăng cường bảo đảm an toàn thông tin mạng.

Địa chỉ hệ thống kỹ thuật tiếp nhận thông tin: https://mis.ais.gov.vn, chi tiết về cổng kết nối và các thông tin khác liên hệ đầu mối kỹ thuật của Cục An toàn thông tin để được hướng dẫn kỹ thuật cụ thể theo thư điện tử: ais@mic.gov.vn; điện thoại: 0242091616.

b) Phương thức kết nối

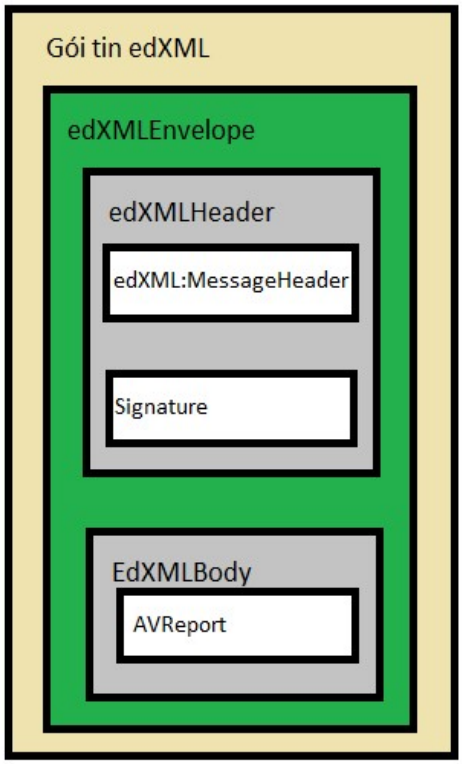
Việc chia sẻ thông tin giữa máy chủ quản lý tập trung của các cơ quan đơn vị với hệ thống kỹ thuật của Bộ Thông tin và Truyền thông được ký số và truyền đi qua kênh mã hoá HTTPS.

Thông tin chia sẻ bao gồm các trường được mô tả trong Phụ lục và đóng gói theo chuẩn edXML.

c) Định dạng thông tin, dữ liệu chia sẻ

Việc kết nối, chia sẻ thông tin giữa các hệ thống kỹ thuật, các hệ thống cần thực hiện trên cơ sở áp dụng định dạng dữ liệu trong gói tin edXML. Mục này quy định các yêu cầu kỹ thuật đối với các trường thông tin của gói tin edXML, không quy định về quy cách đóng gói gói tin edXML. Việc xác định quy cách đóng gói gói tin do các doanh nghiệp cung cấp giải pháp quyết định dựa trên cơ sở đáp ứng được các yêu cầu do các cơ quan có nhu cầu khai thác, sử dụng đặt ra.

Hình 3 mô tả cấu trúc cơ bản của một gói tin edXML gồm hai phần là thông tin cơ bản (edXMLHeader) và thông tin chính (edXMLBody).



Hình 3: Cấu trúc gói tin edXML

Thông tin chi tiết Cấu trúc gói tin edXML tại Phụ lục 4 hướng dẫn này.

4.5.3. Quy trình đăng ký kết nối, chia sẻ dữ liệu về Trung tâm Giám sát an toàn không gian mạng quốc gia

Cơ quan, tổ chức thực hiện quy trình đăng ký kết nối, chia sẻ dữ liệu về Trung tâm Giám sát an toàn không gian mạng quốc gia theo các bước dưới đây:

Bước 1: Các cơ quan, tổ chức gửi văn bản đề nghị kết nối, chia sẻ dữ liệu về Cục An toàn thông tin kèm phiếu đăng ký thông tin theo mẫu tại mục Phụ lục 1 và Phụ lục 2 của tài liệu hướng dẫn này.

Bước 2: Cục An toàn thông tin tiếp nhận thông tin đăng ký của các đơn vị. Trường hợp thông tin nhận được là hợp lệ:

- Đối với kết nối, chia sẻ dữ liệu giám sát an toàn thông tin: Cục An toàn thông tin gửi lại thông tin mã khóa API các điểm giám sát.

- Đối với kết nối, chia sẻ dữ liệu phòng, chống mã độc tập trung: Cục An toàn thông tin thiết lập cấu hình hệ thống cho phép địa chỉ IP của máy chủ chia sẻ dữ liệu kết nối đến máy chủ tiếp nhận dữ liệu của Trung tâm Giám sát an toàn không gian mạng quốc gia.

Bước 3: Các tổ chức, đơn vị thực hiện kết nối chia sẻ dữ liệu và kiểm tra kết nối theo các thông tin do Cục An toàn thông tin cung cấp.

V. NỀN TẢNG QUỐC GIA HỖ TRỢ BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

5.1. Nền tảng hỗ trợ quản lý bảo đảm an toàn hệ thống thông tin theo cấp độ

5.1.1. Giới thiệu chung về nền tảng

a) Giới thiệu chung

Nền tảng hỗ trợ quản lý bảo đảm an toàn hệ thống thông tin theo cấp độ (Nền tảng cấp độ) được xây dựng để hỗ trợ và khuyến nghị cơ quan, tổ chức sử dụng nhằm chuyển đổi số công tác quản lý về bảo đảm an toàn hệ thống thông tin (HTTT) theo cấp độ. Nền tảng cấp độ cung cấp công cụ hỗ trợ xây dựng HSĐXCĐ; quản lý thông tin các HTTT; thống kê và quản lý đồng bộ các số liệu, chỉ tiêu về bảo đảm an toàn HTTT của cả nước, cũng như tại các Bộ, ngành và địa phương. Nền tảng cấp độ hướng đến 02 đối tượng sử dụng:

- Bộ Thông tin và Truyền thông (Cục An toàn thông tin)

Quản lý, nắm bắt kịp thời các thông tin liên quan về công tác bảo đảm an toàn HTTT theo cấp độ của cả nước, đến từng cơ quan, đơn vị như: số lượng, cấp độ HTTT, thông tin về phê duyệt cấp độ; tình hình triển khai phương án bảo đảm an toàn thông tin (ATTT)…

Dễ dàng, thuận tiện trong việc báo cáo số liệu; thông báo, giám sát; cung cấp mẫu HSĐXCĐ, hướng dẫn các quy trình xây dựng, thẩm định và phê duyệt HSĐXCĐ; cung cấp nội dung chỉ đạo, mục tiêu bảo đảm ATTT theo cấp độ…

- Các Bộ, ngành và địa phương (đơn vị chuyên trách, đơn vị vận hành HTTT)

Các đơn vị chuyên trách về ATTT: quản lý, kịp thời báo cáo, cập nhật thông tin, số liệu liên quan đến tình hình xây dựng, phê duyệt HSĐXCĐ…. thuộc phạm vi quản lý.

Các đơn vị vận hành HTTT: xây dựng, cập nhật HSĐXCĐ (Các Hồ sơ mẫu chi tiết; các văn bản, hướng dẫn xây dựng HSĐXCĐ…); cập nhật thông tin, số liệu liên quan đến tình hình xây dựng, phê duyệt HSĐXCĐ… thuộc phạm vi vận hành.

b) Chức năng chính của Nền tảng cấp độ

- Báo cáo tình hình triển khai bảo đảm an toàn thông tin theo cấp độ
- Báo cáo thống kê về Số liệu hệ thống thông tin của cả nước, bộ, ngành, địa phương; Số liệu phê duyệt cấp độ hệ thống thông tin của cả nước, bộ, ngành,

địa phương; Số liệu triển khai phương án bảo đảm an toàn thông tin theo cấp độ của cả nước, bộ, ngành, địa phương; Kế hoạch triển khai xây dựng, phê duyệt hồ sơ đề xuất cấp độ; Kế hoạch triển khai phương án bảo đảm an toàn hệ thống thông tin theo cấp độ

- Thống kê số liệu: Thống kê chi tiết các số liệu về bảo đảm an toàn hệ thống thông tin theo cấp độ của cả nước, bộ, ngành, địa phương; Thống kê số lượng thiết bị, máy chủ, thiết bị dự phòng, hệ thống thông tin thiếu thiết bị dự phòng,…

- Quản lý HTTT

- Hỗ trợ xây dựng Hồ sơ đề xuất cấp độ: Cung cấp tính năng xây dựng HSĐXCĐ trên Nền tảng

- Tài liệu: Cung cấp các Văn bản Quy phạm pháp luật; Hướng dẫn sử dụng Nền tảng; Hồ sơ đề xuất cấp độ mẫu…

5.1.2. Hướng dẫn sử dụng

a) Hướng dẫn đăng ký, kết nối Nền tảng

Để sử dụng Nền tảng, trước hết người dùng đăng nhập vào hệ thống qua tài khoản OneConnect và Nhập mã OTP trên ứng dụng One Connect trên điện thoại thông minh để thực hiện đăng ký và kết nối.

b) Hướng dẫn sử dụng Nền tảng

Đối tượng sử dụng: Đơn vị chuyên trách về an toàn thông tin và đơn vị vận hành.

Nội dung: Hướng dẫn chi tiết người dùng các bước để sử dụng các chức năng về thống kê, báo cáo, xây dựng Hồ sơ đề xuất cấp độ, tài liệu và quản trị tài khoản.

Chi tiết hướng dẫn đăng ký kết nối và sử dụng Nền tảng tại ***Phụ lục 5.***

5.2. Nền tảng điều phối xử lý sự cố an toàn thông tin mạng quốc gia

5.2.1. Giới thiệu chung về Nền tảng

Để nâng cao hiệu quả và hỗ trợ cơ quan, tổ chức trong hoạt động phối hợp ứng cứu sự cố quốc gia, Trung tâm VNCERT/CC thuộc Cục An toàn thông tin đã phát triển Nền tảng điều phối xử lý sự cố an toàn thông tin mạng - IRLab.

Với sứ mệnh nâng cao hiệu quả và tính chuyên nghiệp trong hoạt động của mạng lưới ứng cứu sự cố, Nền tảng IRLab giúp các thành viên mạng lưới UCSC nâng cao tính gắn kết và chia sẻ thông tin, và năng lực phản ứng nhanh trước các mối đe dọa từ không gian mạng. Mục tiêu của IRLab là trở thành địa chỉ uy tín để các cơ quan, tổ chức tìm đến khi gặp sự cố an toàn thông tin. IRLab hoạt động dựa trên triết lý: “Chuyển ứng cứu sự cố từ thế bị động sang chủ động, từ hoạt động đơn lẻ sang hợp tác”.

IRLab cung cấp các dịch vụ như cảnh báo sự cố an toàn thông tin thông qua theo dõi danh sách địa chỉ IP công khai của tổ chức, cập nhật thông tin hàng ngày về lỗ hổng bảo mật mới nhất, các bài phân tích chuyên sâu và các công cụ, kỹ thuật khai thác. Ngoài ra, nền tảng còn hỗ trợ báo cáo sự cố và điều phối, xử lý sự cố từ xa, giúp các tổ chức phản ứng nhanh chóng và hiệu quả hơn trước các nguy cơ an ninh mạng.

Nền tảng được khuyến nghị sử dụng và đối tượng sử dụng là cán bộ kỹ thuật trong hoạt động phối hợp ứng cứu sự cố quốc gia.

5.2.2. Hướng dẫn đăng ký, kết nối Nền tảng

Bước 1: Các tổ chức, doanh nghiệp, cá nhân có nhu cầu sử dụng Nền tảng IRLab khai báo thông tin vào form đăng ký tại địa chỉ: https://irlab.vn/bot hoặc gửi văn bản đăng ký tài khoản IRLab tới Trung tâm VNCERT/CC.

Bước 2: Trung tâm VNCERT/CC sẽ xác nhận thông tin và gửi thông tin phản hồi cho đầu mối đăng ký của tổ chức từ địa chỉ: irlab@vncert.vn.

Chi tiết hướng dẫn đăng ký kết nối và sử dụng Nền tảng tại ***Phụ lục 6.***

5.3. Nền tảng hỗ trợ điều tra số

5.3.1. Giới thiệu chung về Nền tảng

Nền tảng hỗ trợ điều tra số - Digital Forensics Lab (DFLab) nơi tập hợp tri thức và hệ thống, công cụ hỗ trợ phân tích, điều tra tấn công mạng. DFLab được phát triển bởi Trung tâm VNCERT/CC, là một thành phần nằm trong hệ sinh thái của IRLab - Nền tảng điều phối, xử lý sự cố an toàn thông tin mạng quốc gia.

Thông qua DFLab đội ngũ chuyên trách an toàn thông tin tại các cơ quan, tổ chức, doanh nghiệp và cộng đồng an toàn thông tin được huấn luyện các kỹ năng, điều tra với các tình huống tấn công mạng trong thực tế được tái hiện lại một cách khoa học. Đồng thời nền tảng cũng cung cấp hệ thống nghiệp vụ và chuyên biệt để hỗ trợ các tổ chức phân tích, điều tra và xử lý phản hồi nhanh sự cố bảo mật trên diện rộng mà không phụ thuộc khoảng cách địa lý.

Nền tảng được khuyến nghị sử dụng và đối tượng sử dụng là cán bộ kỹ thuật trong hoạt động phân tích, điều tra tấn công mạng.

5.3.2. Hướng dẫn đăng ký, kết nối Nền tảng

Các công cụ, tri thức, tình huống giả định đều được Trung tâm VNCERT/CC chia sẻ công khai thông qua website: https://df.irlab.vn/

Đối với các công cụ online, yêu cầu đăng ký để được hỗ trợ. Quy trình đăng ký như sau:

Bước 1: Các tổ chức, doanh nghiệp có nhu cầu sử dụng Công cụ phân tích online của Nền tảng DFLab, vui lòng gửi văn bản yêu cầu hỗ trợ, cung cấp tài

khoản công cụ của Nền tảng DFLab đến Trung tâm VNCERT/CC. Thông tin trong văn bản bao gồm:

- Chỉ rõ công cụ yêu cầu hỗ trợ, cung cấp tài khoản.

- Mục đích sử dụng công cụ.

- Phạm vi dự kiến áp dụng công cụ trong hoạt động chuyên môn của tổ chức.

Bước 2: Trung tâm VNCERT/CC sẽ xác nhận thông tin và gửi thông tin phản hồi cho đầu mối đăng ký của tổ chức.

5.3.3. Hướng dẫn sử dụng Nền tảng DFLab

Tài liệu hướng dẫn bao gồm các nội dung chính:

- Sổ tay ứng cứu sự cố: Sổ tay ứng cứu sự cố hướng dẫn, đưa ra các bước giải quyết các sự cố trong công việc hoặc tình huống khẩn cấp. Mỗi sổ tay sẽ hướng dẫn các giai đoạn cụ thể thực hiện quy trình ứng cứu sự cố chung và các giai đoạn thực hiện ứng cứu sự cố.

- Bộ công cụ hỗ trợ phân tích: DFLab giới thiệu, hướng dẫn sử dụng các công cụ mã nguồn mở, miễn phí và các công cụ do Trung tâm VNCERT/CC tự phát triển, hỗ trợ việc ứng cứu, điều tra sự cố. Mỗi công cụ được hướng dẫn với các mục sau: Giới thiệu công cụ, các chức năng chính và hướng dẫn sử dụng công cụ. Bộ công cụ này giúp các chuyên gia phát hiện các bằng chứng, dấu hiệu của sự cố, lỗ hổng bảo mật, xác định nguyên nhân của các cuộc tấn công, giúp ứng phó và giải quyết các sự cố nhanh chóng và hiệu quả.

- Hệ thống hỗ trợ phân tích: DFLab cung cấp sẵn sàng các công cụ online sử dụng để phân tích và tra cứu nhật ký, phân tích hành vi mã độc, phân tích nhật ký theo thời gian... để trợ giúp và rút ngắn thời gian ứng cứu sự cố.

- Tình huống giả định: Tình huống huấn luyện của DFLab được xây dựng trên mô hình mạng mô phỏng một doanh nghiệp vừa và nhỏ, đầy đủ các thành phần cơ bản, bao gồm: Vùng mạng server, Vùng mạng người dùng, Vùng mạng tấn công...

Các tình huống của DFLab được xây dựng dựa trên việc mô phỏng các cuộc tấn công mạng nhắm vào nhiều thành phần khác nhau trong hệ thống mạng, thu thập các nhật ký, bằng chứng để người phân tích rà soát, tìm kiếm các dấu hiệu, hành động của kẻ tấn công. Mỗi tình huống bao gồm các mục: Bối cảnh, Câu hỏi, Tệp đính kèm.

Chi tiết hướng dẫn đăng ký kết nối và sử dụng Nền tảng tại ***Phụ lục 7.***

Phụ lục 1
PHIẾU ĐĂNG KÝ THÔNG TIN PHỤC VỤ KẾT NỐI, CHIA SẺ DỮ LIỆU GIÁM SÁT

TÊN CƠ QUAN, TỔ CHỨC **TÊN ĐƠN VỊ**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc** *..., ngày ... tháng ... năm ...*

PHIẾU ĐĂNG KÝ THÔNG TIN

(Chỉ cung cấp cho Cục ATTT để phục vụ kết nối, chia sẻ thông tin với Hệ thống tiếp nhận và xử lý dữ liệu giám sát Quốc gia)

1. Thông tin chung

- Mã đơn vị: [1]
- Tên đơn vị:
- Địa chỉ:
- Số điện thoại:
- Email:
- Đơn vị cung cấp dịch vụ:
- Đại diện hợp pháp của cơ quan/tổ chức *(nếu có)*:
  + Họ và tên:
  + Email:
- Đầu mối kỹ thuật của cơ quan/tổ chức:
  + Họ và tên:
  + Số điện thoại:
  + Email:

[1] Nhập mã định danh điện tử của cơ quan/tổ chức/doanh nghiệp *(theo quyết định số 20/2020/QĐ-TTg của Thủ tướng Chính phủ)*, ví dụ:

- Cơ quan/Tổ chức: **Sở TTTT tỉnh An Giang**, có mã định danh điện tử là **H01.07**
- Doanh nghiệp: **Tập đoàn Điện lực Việt Nam**, có mã định danh điện tử là **100100079**

2. Thông tin các điểm chia sẻ dữ liệu sát giám

- Điểm chia sẻ số 1:
  + Tên địa điểm: [2]
  + Địa chỉ:
  + Đơn vị cung cấp dịch vụ:
- Điểm chia sẻ số …:
  + Tên địa điểm:
  + Địa chỉ:
  + Đơn vị cung cấp dịch vụ:

Ghi chú: *Bản mềm gửi về hòm thư soc@ais.gov.vn, cc: ncsc@ais.gov.vn*

ĐẠI DIỆN LÃNH ĐẠO ĐƠN VỊ
(Ghi rõ chức danh, họ tên, ký và đóng dấu)

[2] Nhập tên đơn vị cài đặt sensor giám sát, ví dụ: **Cục An toàn thông tin**

Phụ lục 2
PHIẾU ĐĂNG KÝ THÔNG TIN PHỤC VỤ KẾT NỐI, CHIA SẺ DỮ LIỆU PHÒNG, CHỐNG MÃ ĐỘC

TÊN CƠ QUAN, TỔ CHỨC **TÊN ĐƠN VỊ**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc** *..., ngày ... tháng ... năm ...*

PHIẾU ĐĂNG KÝ THÔNG TIN

(Chỉ cung cấp cho Cục ATTT để phục vụ kết nối, chia sẻ thông tin với Hệ thống tiếp nhận và xử lý dữ liệu mã độc Quốc gia)

1. Thông tin chung

- Mã đơn vị: [3]
- Tên đơn vị:
- Địa chỉ:
- Số điện thoại:
- Email:
- Đơn vị cung cấp dịch vụ:
- Đại diện hợp pháp của cơ quan/tổ chức *(nếu có)*:
  + Họ và tên:
  + Email:
- Đầu mối kỹ thuật của cơ quan/tổ chức:
  + Họ và tên:
  + Số điện thoại:
  + Email:

[3] Nhập mã định danh điện tử của cơ quan/tổ chức/doanh nghiệp *(theo quyết định số 20/2020/QĐ-TTg của Thủ tướng Chính phủ)*, ví dụ:

- Cơ quan/Tổ chức: **Sở TTTT tỉnh An Giang**, có mã định danh điện tử là **H01.07**
- Doah nghiệp: **Tập đoàn Điện lực Việt Nam**, có mã định danh điện tử là **100100079**

Thông tin các điểm chia sẻ dữ liệu mã độc

- Điểm chia sẻ số 1:
  + Tên địa điểm: [4]
  + Địa chỉ:
  + Tên giải pháp phòng chống mã độc được cài đặt:
  + Số lượng máy được cài đặt thực tế:
  + Địa chỉ IP public của điểm chia sẻ:
- Điểm chia sẻ số ...:
  + Tên địa điểm:
  + Địa chỉ:
  + Tên giải pháp phòng chống mã độc được cài đặt:
  + Số lượng máy được cài đặt thực tế:
  + Địa chỉ IP public của điểm chia sẻ:

Ghi chú: *Bản mềm gửi về hòm thư soc@ais.gov.vn, cc: ncsc@ais.gov.vn*

ĐẠI DIỆN LÃNH ĐẠO ĐƠN VỊ
(Ghi rõ chức danh, họ tên, ký và đóng dấu)

[4] Nhập tên đơn vị cài đặt giải pháp phòng chống mã độc, ví dụ: **Cục An toàn thông tin**

Phụ lục 3
ĐỊNH DẠNG DỮ LIỆU CHIA SẺ DỮ LIỆU GIÁM SÁT AN TOÀN THÔNG TIN MẠNG

STT	Tên trường	Định dạng dữ liệu	Mô tả	Thuộc tính	Ghi chú
1	vendor_id	string	Mã tổ chức thực hiện giám sát. Mã này do Cục An toàn thông tin cung cấp sau khi tổ chức đăng ký tài khoản.	Bắt buộc	
2	unit_id	string	Mã tổ chức được giám sát. Mã này do Cục An toàn thông tin cung cấp sau khi tổ chức đăng ký tài khoản.	Bắt buộc	QCVN 102:2016/BTTTT
3	sensor_id	string	Mã sensor, Mã này do Cục An toàn thông tin cung cấp sau khi tổ chức đăng ký tài khoản.	Bắt buộc	Đây là thiết bị hoặc hệ thống giám sát (sensor) chia sẻ dữ liệu về Hệ thống tiếp nhận và xử lý dữ liệu giám sát Quốc gia.
4	timestamp	float	Thời gian mà sensor ghi nhận được sự kiện.	Bắt buộc	Sử dụng định dạng UNIX Time
5	category	number	Phân loại cảnh báo vào loại hình tấn công	Bắt buộc	Category được phân loại theo chuẩn của chuẩn của MITRE

STT	Tên trường	Định dạng dữ liệu	Mô tả	Thuộc tính	Ghi chú
					1: Initial Access 2: Execution 3: Persistence 4: Privilege Escalation 5: Defense Evasion 6: Credential Access 7: Discovery 8: Lateral Movement 9: Collection 10: Command and Control 11: Exfiltration 12: Impact Tham khảo https://attack.mitre.org/matrices/enterprise/
6	action	number	Hành động của sensor đối với gói tin. *Ví dụ: Allowed là cho phép gói tin được đi qua*	Bắt buộc	1: Allowed 2: Drop 3: Alerted 4: Suspended 5: Archived 6: Other

STT	Tên trường	Định dạng dữ liệu	Mô tả	Thuộc tính	Ghi chú
7	signature	string	Dấu hiệu nhận biết liên quan đến cảnh báo	Bắt buộc	Định dạng Signature tùy thuộc vào từng nhà chung cấp dịch vụ giám sát. Khuyến nghị chia sẻ thông tin chi tiết, tuy nhiên có thể chia sẻ thông tin mô tả.
8	severity	number	Mức độ nghiêm trọng/ưu tiên của cảnh báo Khuyến nghị chỉ chia sẻ cảnh báo từ mức 2 đến mức 4	Bắt buộc	1: Low 2: Medium 3: High 4: Critical
9	direction	number	Hướng của gói tin	Bắt buộc	0: outbound 1: inbound 2: local
10	dest_ip	string	Địa chỉ IP đích của gói tin	Bắt buộc	
11	dest_port	number	Địa chỉ cổng đích của gói tin	Bắt buộc	
12	src_ip	string	Địa chỉ IP nguồn của gói tin	Bắt buộc	
13	src_port	number	Địa chỉ cổng nguồn của gói tin	Bắt buộc	
14	proto	string	Giao thức sử dụng để truyền tải	Bắt buộc	Chiều dài từ 2-10 ký tự

STT	Tên trường	Định dạng dữ liệu	Mô tả	Thuộc tính	Ghi chú
			gói tin		HTTP, TCP, DNS, UNDEFINED
15	domain	string	Tên miền của máy chủ điều khiển C&C	Tùy chọn	
16	host	string	Tên của sensor	Bắt buộc	
17	data_leak	[string]	Danh sách dữ liệu bị lộ, lọt	Tùy chọn	
18	tags	number	Trường thông tin về geoip	Bắt buộc	1: có tìm thấy geoip, 0: không tìm thấy geoip
19	geoip	object	Vị trí địa lý của IP public (có thể là địa chỉ nguồn hoặc địa chỉ đích của gói tin) không thuộc hệ thống được giám sát. Giá trị này phụ thuộc vào trường tags. Chỉ khi trường tags trả về giá trị 1 thì mới có các thuộc tính của đối tượng này. Các trường hợp khác các thuộc tính là NULL.	Tùy chọn	

STT	Tên trường	Định dạng dữ liệu	Mô tả	Thuộc tính	Ghi chú
19.1	lat	number	Vĩ độ	Bắt buộc	
19.2	lon	number	Kinh độ	Bắt buộc	
19.3	ip	string	Địa chỉ IP public (có thể là địa chỉ nguồn hoặc địa chỉ đích của gói tin) không thuộc hệ thống được giám sát.	Bắt buộc	
19.4	city_name	string	Tên thành phố	Bắt buộc	
19.5	country_name	string	Tên quốc gia	Bắt buộc	
19.6	country_code	string	Mã quốc gia theo chuẩn mới nhất	Bắt buộc	
19.7	timezone	string	Múi giờ	Bắt buộc	
19.8	region_name	string	Tên vùng	Bắt buộc	

Phụ lục 4
ĐỊNH DẠNG DỮ LIỆU CHIA SẺ DỮ LIỆU VỀ MÃ ĐỘC

1. PHẦN SOAP-ENV:HEADER

STT	Tên trường	Định dạng dữ liệu	Mô tả	Thuộc tính	Ghi chú
1.	**edXML:MessageHeader**		Đây là thông tin phải có của phần đầu gói tin, lưu trữ các thông tin về phần mở đầu và phần kết thúc của một báo cáo.	Bắt buộc	
1.1	edXML:From		Thông tin về đối tượng gửi báo cáo	Bắt buộc	
1.1.1	*edXML:OrganId*	Kiểu String Độ dài tối đa: 13	ID của cơ quan, tổ chức gửi báo cáo	Bắt buộc	QCVN 102:2016/BTTTT
1.1.2	*edXML:OrganizationInCharge*	Kiểu String Độ dài tối đa: 200	Tên cơ quan, tổ chức chủ quản trực tiếp (nếu có)	Tùy chọn	

STT	Tên trường	Định dạng dữ liệu	Mô tả	Thuộc tính	Ghi chú
1.1.3	*edXML:OrganName*	Kiểu String Độ dài tối đa: 200	Tên cơ quan, tổ chức gửi báo cáo	Bắt buộc	
1.1.4	*edXML:OrganAdd*	Kiểu String Độ dài tối đa: 250	Địa chỉ của cơ quan, tổ chức gửi báo cáo	Bắt buộc	
1.1.5	*edXML:Email*	Kiểu String Độ dài tối đa: 100	Thư điện tử liên lạc của cơ quan, tổ chức gửi báo cáo	Bắt buộc	
1.1.6	*edXML:Telephone*	Kiểu String Độ dài tối đa: 20	Số điện thoại của cơ quan, tổ chức gửi báo cáo	Bắt buộc	
1.1.7	*edXML:Fax*	Kiểu String Độ dài tối đa: 20	Số fax của cơ quan, tổ chức gửi báo cáo	Tùy chọn	
1.1.8	*edXML:Website*	Kiểu String Độ dài tối đa: 100	Trang/cổng thông tin điện tử của cơ quan, tổ chức gửi báo cáo	Tùy chọn	

STT	Tên trường	Định dạng dữ liệu	Mô tả	Thuộc tính	Ghi chú
1.2	edXML:Subject	Kiểu String Độ dài tối đa: 500	Trích yếu nội dung của báo cáo	Bắt buộc	
2	**Signature**		Mô tả về chữ ký số và thông tin ký số gói tin edXML	Bắt buộc	
2.1	*SignedInfo*		Mô tả các thông tin được ký số	Bắt buộc	
2.1.1	*CanonicalizationMethod*		Xác định thuật toán chuẩn hóa dữ liệu cần ký số	Bắt buộc	Là một thuộc tính của *Canonicalization Method*
	Algorithm	Kiểu String	Thuật toán chuẩn hóa dữ liệu: http://www.w3.org/TR/xml-exc-c14n/		
2.1.2	*SignatureMethod*		Xác định thuật toán để ký số thành phần *SignedInfo* đã được chuẩn hóa	Bắt buộc	
	Algorithm	Kiểu String	Thuật toán ký số *SignedInfo*: http://www.w3.org/2000/09/xmldsi		Là một thuộc tính của

STT	Tên trường	Định dạng dữ liệu	Mô tả	Thuộc tính	Ghi chú
			g#rsa-sha1		*SignatureMethod*
2.1.3	*Reference*		Tham chiếu đến các đối tượng dữ liệu cần ký và xác định phương thức băm và giá trị băm của các thành phần đối tượng dữ liệu trong gói tin edXML	Bắt buộc	
	URI	Kiểu String	Tham chiếu đến đối tượng dữ liệu được băm. URI = "" tham chiếu đến *SOAP-ENV:Envelope*. URI = cid tham chiếu đến từng tệp dữ liệu đính kèm		Là một thuộc tính của *Reference*
2.1.3.1	*Transforms*		Danh sách phương thức biến đổi đối tượng dữ liệu định dạng XML được tham chiếu trước khi ký số	Bắt buộc	Chỉ sử dụng *Transforms* với đối tượng SOAP-ENV:Envelope (XML)
	Transform		Định nghĩa một phương thức biến đổi sẽ được áp dụng	Bắt buộc	
	Algorithm	Kiểu String	Tên phương thức biến đổi được áp		Là một thuộc tính

STT	Tên trường	Định dạng dữ liệu	Mô tả	Thuộc tính	Ghi chú
			dụng. Có các loại sau: - Sử dụng Enveloped Signature: www.w3.org/2000/09/XMLDSig#enveloped-signature - Sử dụng thuật toán chuẩn hóa nội dung XML, XML-C14N: www.w3.org/TR/xml-exc-c14n/		của *Transforms*
2.1.3.2	*DigestMethod*		Xác định thuật toán băm dữ liệu http://www.w3.org/2001/04/xmlenc#sha256	Bắt buộc	
	Algorithm	Kiểu String	Thuật toán băm dữ liệu		Là một thuộc tính của *DigestMethod*
2.1.3.3	*DigestValue*	Kiểu String	Giá trị băm của đối tượng dữ liệu tham chiếu sử dụng thuật toán quy định tại *DigestMethod*	Bắt buộc	
2.2	*SignatureValue*	Kiểu String	Giá trị chữ ký số của *SignedInfo*	Bắt buộc	

STT	Tên trường	Định dạng dữ liệu	Mô tả	Thuộc tính	Ghi chú
2.3	*KeyInfo*		Mô tả khóa sử dụng để xác thực chữ ký số	Bắt buộc	
2.3.1	*X509Data*		Dữ liệu về chứng thư số sử dụng để xác thực chữ ký số	Bắt buộc	
2.3.1.1	*X509SubjectName*	Kiểu String	Tên cá nhân/tổ chức ký số	Bắt buộc	Tên cá nhân/tổ chức sở hữu chứng thư số ký
2.3.1.2	*X509Certificate*	Kiểu String	Chứng thư số sử dụng để xác thực chữ ký số	Bắt buộc	

2. Phần SOAP-ENV: Body

STT	Tên trường	Định dạng dữ liệu	Mô tả	Thuộc tính	Ghi chú
1	**AVReport**		Các thông tin báo cáo của Anti Virus	Bắt buộc	

STT	Tên trường	Định dạng dữ liệu	Mô tả	Thuộc tính	Ghi chú
	name	Kiểu String	Tên của Anti Virus gửi báo cáo	Bắt buộc	
1.1	**Datetime**	Kiểu string	Thời gian gửi báo cáo	Bắt buộc	Sử dụng Unix time
1.2	**Malware**		Báo cáo thông tin mã độc trên các máy	Bắt buộc	Nếu không có mã độc thì nội dung bỏ trống, nếu có thì **bắt buộc** phải có các thẻ bên trong.
1.2.1	**Machine**		Thông tin về mã độc trên từng máy	Bắt buộc	Bỏ qua nếu không có thông tin mã độc
	ip	Kiểu string	Địa chỉ IP của máy nhiễm mã độc	Bắt buộc	Bỏ qua nếu không có thông tin mã độc
	ippublic	Kiểu string	Địa chỉ IP public của máy tính bị nhiễm mã độc	Tuỳ chọn	Bỏ qua nếu không có thông tin mã độc
	name	Kiểu string	Tên máy nhiễm mã độc	Bắt buộc	Bỏ qua nếu không có thông tin mã độc
1.2.1.1	**MalwareInfo**		Các thông tin về mã độc trên máy	Bắt buộc	Bỏ qua nếu không có thông tin mã độc
1.2.1.1.1	**MalwareName**	Kiểu string	Tên mã độc	Bắt buộc	Bỏ qua nếu không có thông tin

STT	Tên trường	Định dạng dữ liệu	Mô tả	Thuộc tính	Ghi chú
					mã độc
1.2.1.1.2	**MalwareType**	Kiểu string	Loại mã độc (PE, Trojan, spyware, worm, …)	Bắt buộc	Bỏ qua nếu không có thông tin mã độc
1.2.1.1.3	**MalwareBehavior**	Kiểu string	Hành vi của mã độc (Downloader, Dropper, CoinMiner, Keylogger, …)	Bắt buộc	Bỏ qua nếu không có thông tin mã độc
1.2.1.1.4	**TypeOfDevice**	Kiểu string	Loại thiết bị nhiễm mã độc (USB, HDD, SDCard, SSD, …)	Bắt buộc	Bỏ qua nếu không có thông tin mã độc
1.2.1.1.5	**NumberFile**	Kiểu integer	Số lượng tập tin bị nhiễm mã độc	Bắt buộc	Bỏ qua nếu không có thông tin mã độc
1.3	**Connection**		Thông tin kết nối nghi ngờ.	Bắt buộc	Nếu không có connection lạ thì các trường bên trong bỏ trống. Nếu có thông tin Connection thì các trường bên trong **bắt buộc** phải có.
1.3.1	**Machine**		Thông tin kết nối nghi ngờ trên	Bắt buộc	Bỏ qua nếu không có thông tin

STT	Tên trường	Định dạng dữ liệu	Mô tả	Thuộc tính	Ghi chú
			từng máy		connection
	ip	Kiểu string	IP của máy có kết nối nghi ngờ	Bắt buộc	Bỏ qua nếu không có thông tin connection
	ippublic	Kiểu string	Địa chỉ IP public của máy tính bị nhiễm mã độc	Tuỳ chọn	
	name	Kiểu string	Tên của máy có kết nối nghi ngờ.	Bắt buộc	Bỏ qua nếu không có thông tin connection
1.3.1.1	**ConnectionInfo**		Thông tin kết nối nghi ngờ	Bắt buộc	Bỏ qua nếu không có thông tin connection
1.3.1.1.1	**Program**	Kiểu string	Tên chương trình có kết nối nghi ngờ.	Bắt buộc	Bỏ qua nếu không có thông tin connection
1.3.1.1.2	**TargetIP**	Kiểu string	IP đích của kết nối nghi ngờ.	Tuỳ chọn	Bỏ qua nếu không có thông tin connection
1.4	**Vulnerability**		Thông tin lỗ hổng trên các máy	Bắt buộc	Nếu không có lỗ hổng nào trên các máy thì các trường bên trong bỏ trống. Nếu có lỗ hổng

STT	Tên trường	Định dạng dữ liệu	Mô tả	Thuộc tính	Ghi chú
					thì các trường bên trong **bắt buộc** phải có.
1.4.1	**Machine**		Thông tin lỗ hổng trên từng máy	Bắt buộc	Bỏ qua nếu không có thông tin lỗ hổng.
	ip	Kiểu string	Địa chỉ IP của máy có lỗ hổng	Bắt buộc	Bỏ qua nếu không có thông tin lỗ hổng.
	ippublic	Kiểu string	Địa chỉ IP public của máy tính có lỗ hổng	Tuỳ chọn	Bỏ qua nếu không có thông tin lỗ hổng
	name	Kiểu string	Tên của máy có lỗ hổng	Bắt buộc	Bỏ qua nếu không có thông tin lỗ hổng.
1.4.1.1	**VulnerabilityInfo**		Các thông tin về lỗ hổng	Bắt buộc	Bỏ qua nếu không có thông tin lỗ hổng.
1.4.1.1.1	**Name**	Kiểu string	Mã CVE của lỗ hổng	Bắt buộc	Bỏ qua nếu không có thông tin lỗ hổng.
1.4.1.1.2	**OSName**	Kiểu string	Tên hệ điều hành của máy có lỗ hổng	Tuỳ chọn	Bỏ qua nếu không có thông tin lỗ hổng.

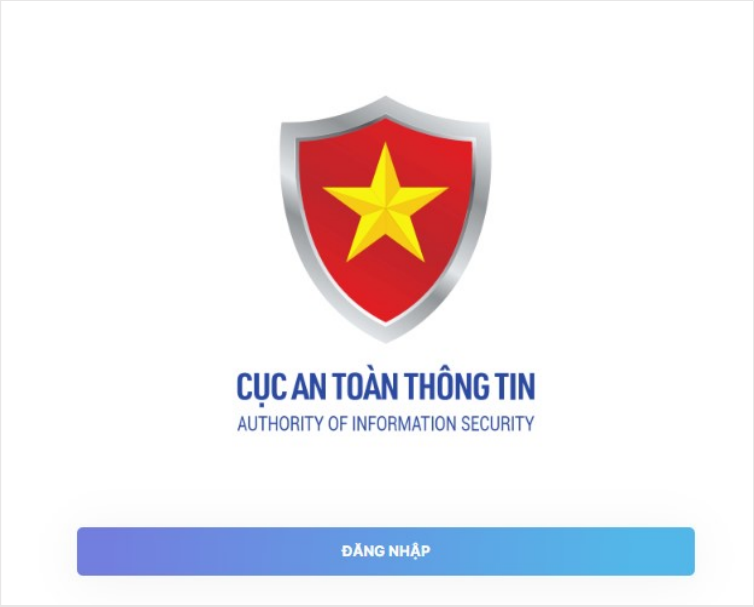
STT	Tên trường	Định dạng dữ liệu	Mô tả	Thuộc tính	Ghi chú
1.5	**OS**		Thông tin hệ điều hành của các máy	Bắt buộc	
1.5.1	**Machine**		Máy có báo cáo thông tin hệ điều hành	Bắt buộc	
	ip	Kiểu string	IP của máy có báo cáo thông tin hệ điều hành	Bắt buộc	
	ippublic	Kiểu string	Địa chỉ IP public của máy tính có báo cáco thông tin hệ điều hành	Tuỳ chọn	
	name	Kiểu string	Tên của máy có báo cáo thông tin hệ điều hành	Bắt buộc	
1.5.1.1	**OSName**	Kiểu string	Tên hệ điều hành	Bắt buộc	
1.5.1.2	**LastUpdate**	Kiểu string	Thời gian cập nhật hệ điều hành mới nhất	Bắt buộc	Định dạng Unix time
1.6	**Update**		Thông tin tình hình cập nhật của các máy	Bắt buộc	
1.6.1	**NumberMachineNot**	Kiểu	Số máy không được cập nhật	Bắt buộc	Tất cả máy được update ≤ 15

STT	Tên trường	Định dạng dữ liệu	Mô tả	Thuộc tính	Ghi chú
	UpdateOn15Day	Interger	trong vòng 15 ngày.		ngày thì dữ liệu ghi 0.
1.7	**QualityFeature**		Thông tin trạng thái bật tắt của những tính năng quan trọng	Bắt buộc	
1.7.1	**Machine**		**Máy có báo có thông tin trạng thái bật tắt của những tính năng quan trọng**		
	ip	Kiểu string	IP của máy	Bắt buộc	
	Name	Kiểu string	Tên máy	Bắt buộc	
1.7.1.1	**AutoProtect**	Kiểu string	Trạng thái tính năng tự động bảo vệ thời gian thực (On, Off)	Bắt buộc	
1.7.1.2	**EnableFirewall**	Kiểu string	Trạng thái của firewall (On, Off)	Bắt buộc	

Phụ lục 5
HƯỚNG DẪN SỬ DỤNG NỀN TẢNG HỖ TRỢ QUẢN LÝ BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN THEO CẤP ĐỘ

1. Hướng dẫn đăng ký, kết nối Nền tảng

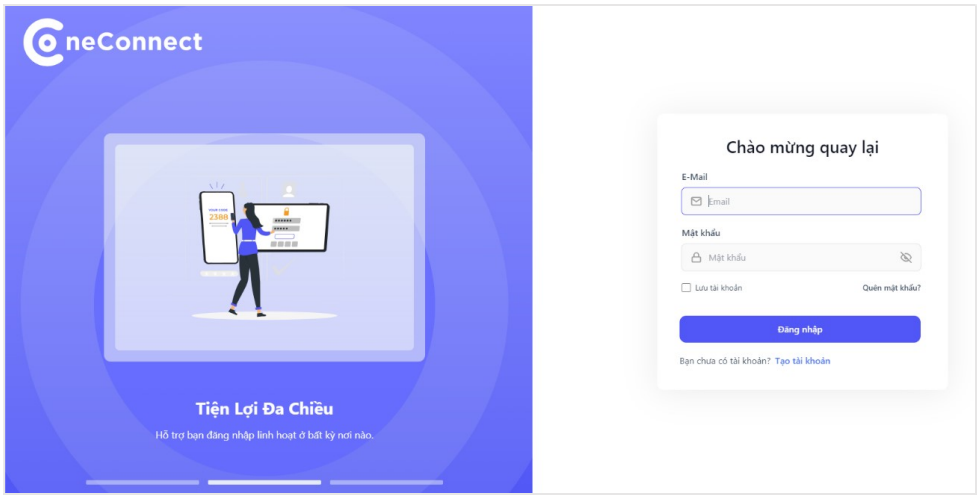
Bước 1: Người dùng đăng nhập hệ thống qua đường dẫn ***https://capdo.ais.gov.vn/***. Chọn nút "Đăng nhập" ở góc trên bên phải màn hình.



Hình 1: Màn đăng nhập hệ thống

Sau đó, nhấn vào nút "Đăng nhập"

Bước 2: Người dùng đăng nhập hệ thống bằng tài khoản oneconnect đã đăng ký và được cấp.



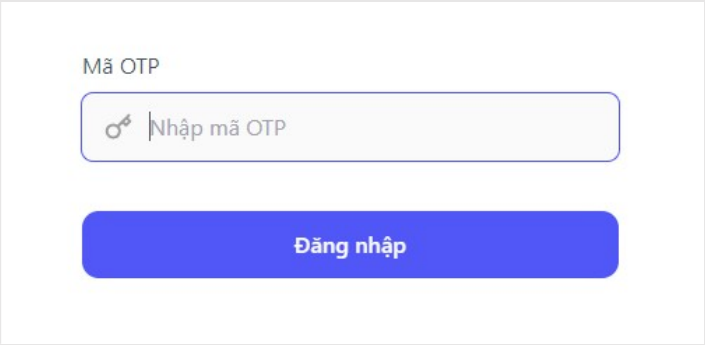
Hình 2: Màn kết nối Oneconnect

- **"Email"**: Nhập tên email đã đăng ký

- **"Mật khẩu"**: Nhập mật khẩu

Bước 3: Nhấn nút ĐĂNG NHẬP để đăng nhập vào hệ thống qua tài khoản OneConnect

Bước 4: Nhập mã OTP trên ứng dụng One Connect trên điện thoại thông minh



Hình 3: Màn nhập mã OTP

Sau đó nhấn "Đăng nhập" là đã có thể vào sử dụng tài khoản đã được đăng ký.

2. Hướng dẫn sử dụng nền tảng

2.1. Đối với tài khoản Đơn vị chủ quản

a) Chức năng Thống kê

Mục đích: Để người dùng có thể nắm bắt được thông tin số liệu, tỷ lệ phê duyệt HTTT qua những biểu đồ thống kê.

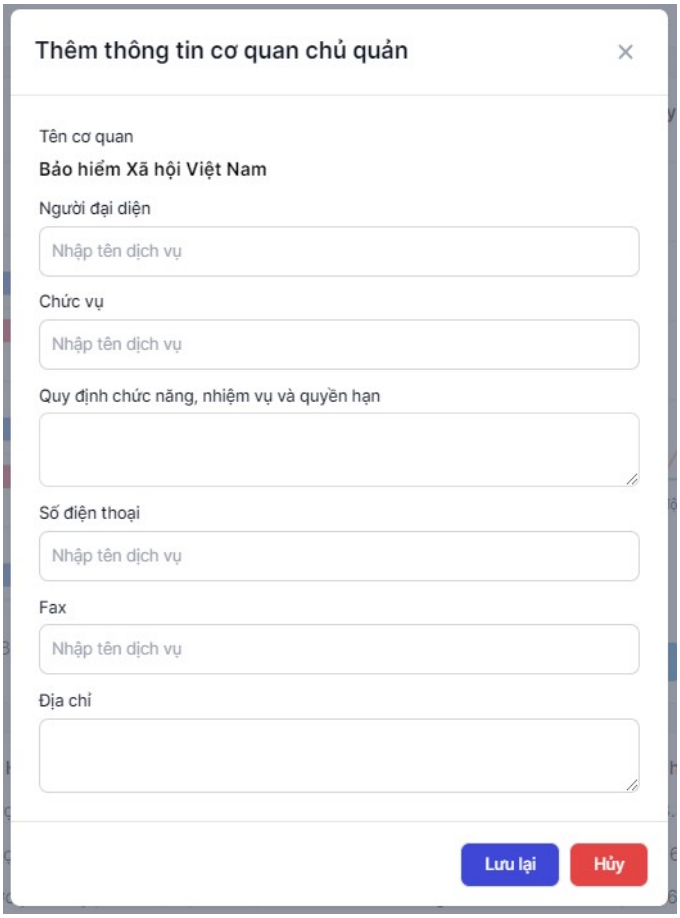
Thao tác:

Bước 1: Từ menu trái chọn Dashboard để chuyển đến màn "**Biểu đồ thống kê HTTT**"

Bước 2: Màn "**Biểu đồ thống kê HTTT**" hiển thị thống kê tỷ lệ phê duyệt , số liệu phê duyệt HTTT với cả nước

Hình 4: Màn biểu đồ thống kê số liệu HTTT

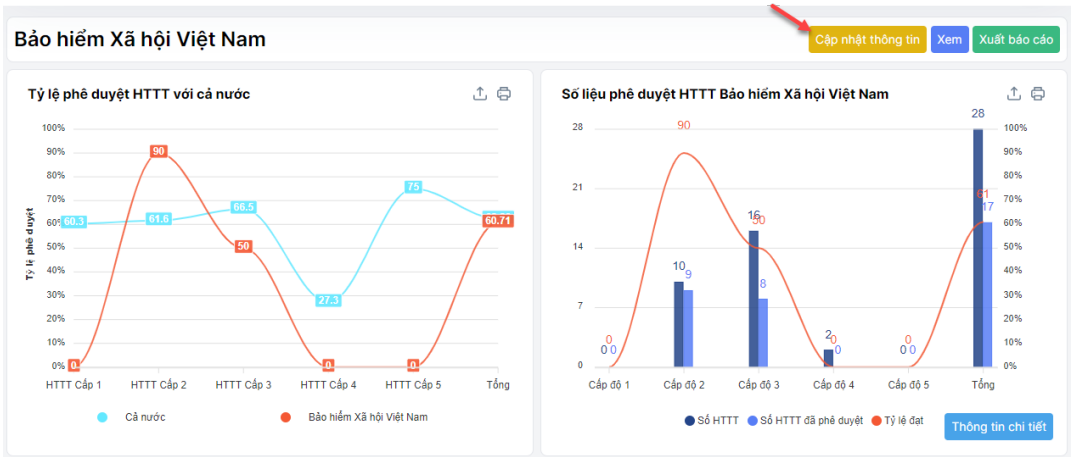
Bước 3: Có thể Thêm thông tin cơ quan chủ quản



Hình 5: Màn nhập thông tin đơn vị chủ quản

Điền thông tin đầy đủ xong chọn lưu lại để lưu thông tin vừa nhập

Bước 4: Sau khi nhập xong thông tin người dùng có thể cập nhật bằng cách chọn: "Cập nhật thông tin"

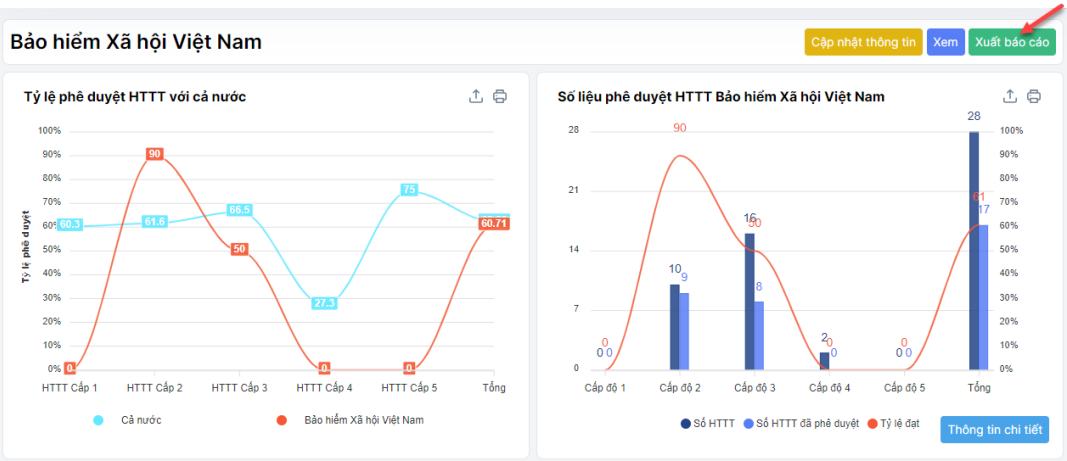


Hình 6: Màn biểu đồ thống kê số liệu HTTT

Hoặc xem thông tin

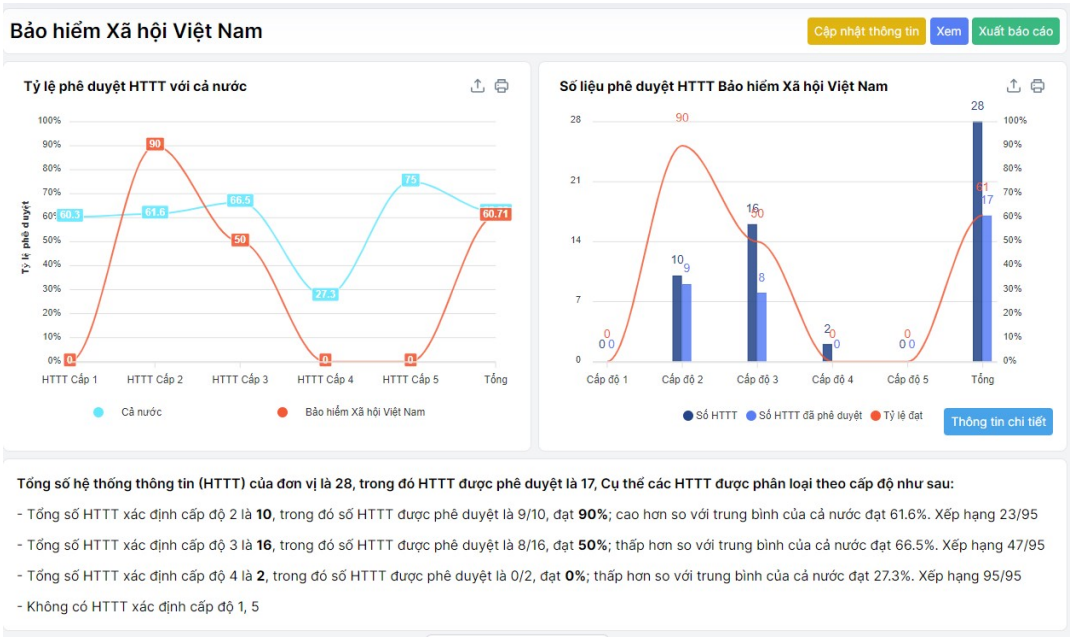
Hình 7: Màn biểu đồ thống kê số liệu HTTT

Người dùng cũng có thể xuất thông tin bằng cách Xuất báo cáo



Hình 8: Màn biểu đồ thống kê số liệu HTTT

Bước 5: Chọn Thông tin chi tiết thông tin chi tiết số liệu phê duyệt HTTT sẽ được hiển thị đầy đủ bên dưới



Hình 9: Màn biểu đồ thống kê số liệu HTTT

b) Chức năng Báo cáo, thống kê

Chức năng cho phép người dùng tạo mới, gửi và quản lý danh sách các số liệu hệ thống thông tin đã thống kê

Báo cáo số liệu

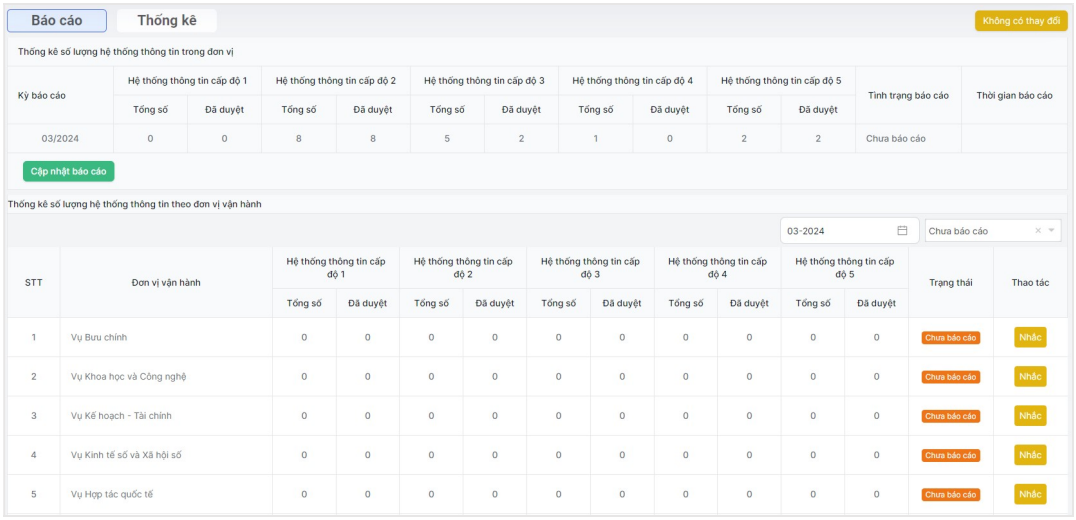
Mục đích: Hiển thị thống kê số lượng HTTT trong đơn vị, tình trạng báo cáo theo các kỳ của đơn vị. Người dùng các đơn vị có thể gửi báo cáo số liệu HTTT lên cục ATTT phụ trách

Thao tác:

Bước 1: Từ menu trái chọn 

để chuyển đến màn "Báo cáo số liệu hệ thống thông tin"

Bước 2: Màn "**Báo cáo số liệu hệ thống thông tin**" hiển thị thống kê số liệu HTTT trong đơn vị danh sách HTTT trong đơn vị.

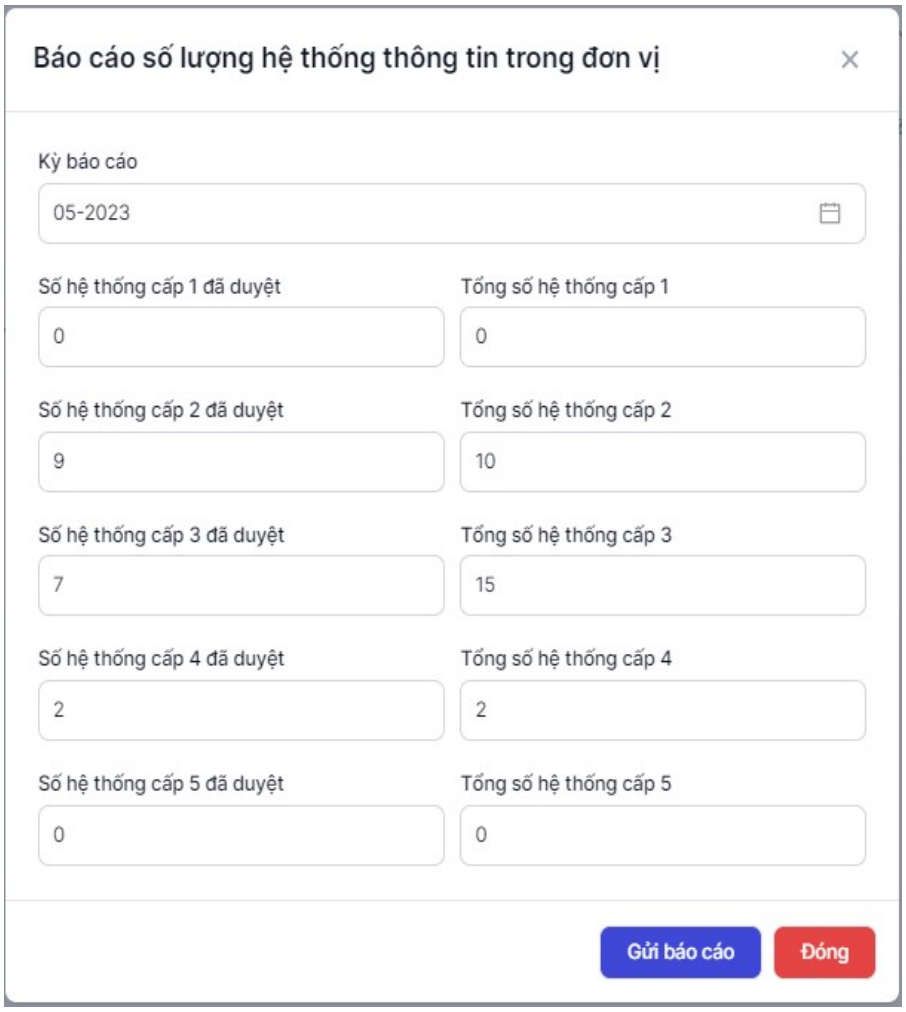


Hình 10: Màn thống kê số liệu HTTT và danh sách HTTT trong đơn vị

Bước 3: Chọn Cập nhật báo cáo để gửi số liệu báo cáo lên đơn vị phụ trách(Cục ATTT)

Bước 4: Nếu kỳ báo cáo không có thay đổi so với kỳ trước, chọn Không có thay đổi để gửi báo

cáo. Số liệu được tính tự động theo danh sách HTTT của đơn vị. Chọn Gửi báo cáo để gửi số liệu báo cáo lên đơn vị phụ trách(Cục ATTT)



Hình 11: Màn minh họa báo cáo không có thay đổi

Thống kê đơn vị

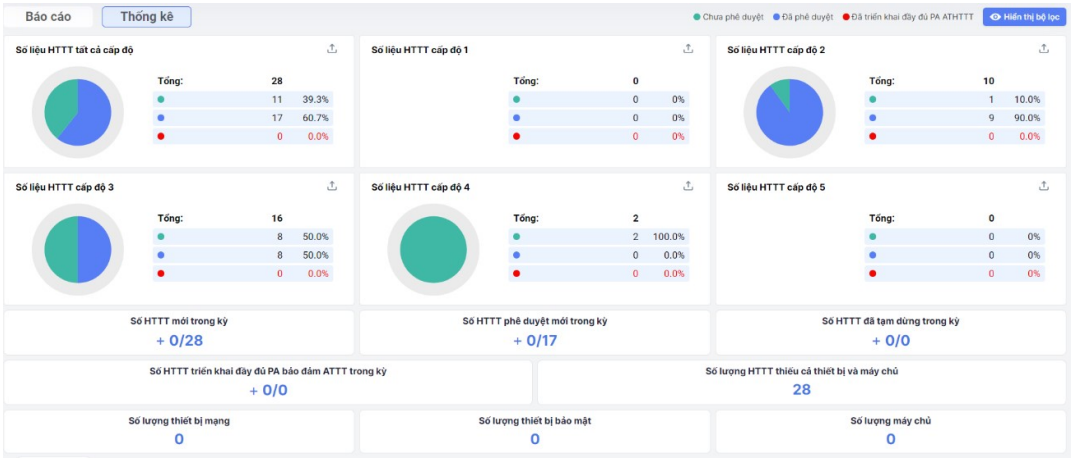
Mục đích: Cung cấp thông tin thống kê số lượng, thiết bị, máy chủ, phê duyệt mới, triển khai HTTT trong đơn vị

Thao tác:

Bước 1: Từ menu trái chọn 

để chuyển đến màn "**Thống kê hệ thống thông tin**"

Bước 2: Màn "**Thống kê hệ thống thông tin**" hiển thị thống kê , số liệu HTTT trong đơn vị.



Hình 12: Màn thống kê HTTT .

c) Chức năng Quản lý hệ thống thông tin

Danh sách hệ thống thông tin

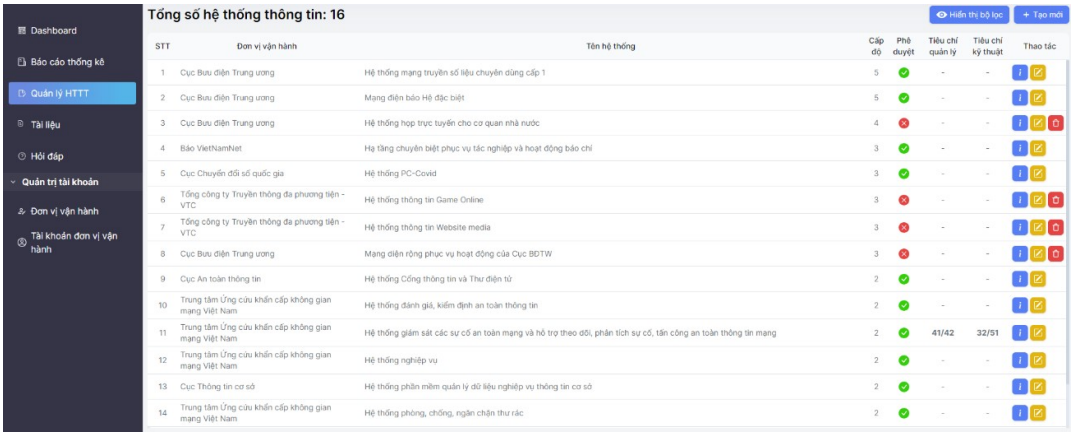
Mục đích: Chức năng này giúp người dùng xem tổng thể danh sách HTTT trong đơn vị, tìm kiếm HTTT theo tên hoặc theo cấp độ HTTT

Thao tác:

Bước 1: Từ màn hình "**Quản lý người dùng**" chọn nút 

để chuyển đến màn danh sách HTTT

Bước 2: Tại màn hình "**Danh sách hệ thống thông tin**" hiển thị tổng thể danh sách HTTT trong đơn vị.



Hình 13: Màn danh sách hệ thống thông tin

- Người dùng có thể lọc danh sách HTTT theo các cấp độ hệ thống, đơn vị vận hành, trạng thái phê duyệt, thông tin hiện trạng, tình trạng triển khai đầy đủ phương án ATTT, hoặc tra cứu theo tên HTTT

Hình 14: Mục tra cứu danh sách hệ thống thông tin

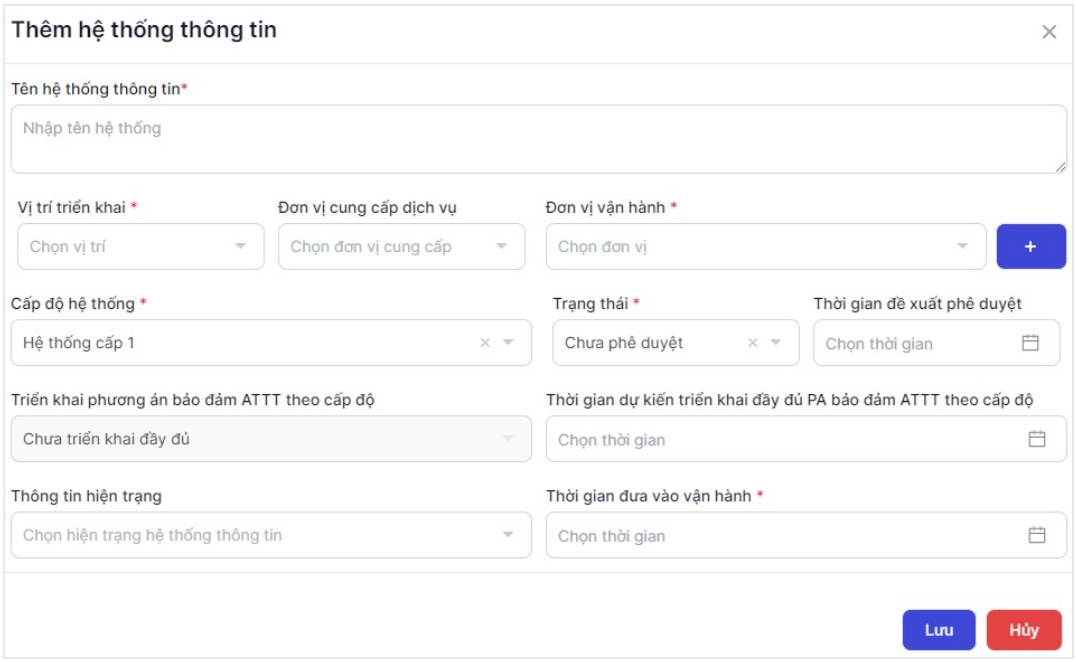
Người dùng cũng có thể xem thông tin chi tiết HTTT, chọn để cập nhật thông tin HTTT hoặc chọn để chuyển HTTT sang danh sách dừng vận hành, hoặc để vận hành lại HTTT

Thêm mới hệ thống thông tin

Mục đích: Chức năng này giúp người dùng thêm mới HTTT

Thao tác:

Bước 1: Từ menu bên trái chọn Danh mục Hệ thống, người dùng di chuyển sang tay phải màn hình chọn + Tạo mới để người dùng nhập các thông tin về HTTT cần tạo



Hình 15: Màn thêm mới hệ thống thông tin

- **"Tên hệ thống thông tin"**: Nhập tên của HTTT
- **"Vị trí triển khai"**: Nhập vị trí triển khai hệ thống(Tại cơ sở hoặc thuê dịch vụ)
- **"Đơn vị cung cấp dịch vụ"**: chọn đơn vị cung cấp nếu hệ thống triển khai tại doanh nghiệp
- **"Đơn vị vận hành"**: Nhập tên đơn vị vận hành hệ thống
- **"Cấp độ hệ thống"**: Chọn cấp độ của hệ thống

- **"Trạng thái"**: Nhập trạng thái phê duyệt hệ thống
- **"Thời gian đề xuất"**: Nhập thời gian đề xuất nếu hệ thống chưa phê duyệt
- **"Thời gian dự kiến triển khai đầy đủ PA ATTT"**: Nhập thời gian dự kiến
- **"Thông tin hiện trạng "**: Chọn hiện trạng hệ thống thông tin
- **"Thời gian đưa vào vận hành"**: Người dùng chọn thời gian bắt đầu sử dụng hệ thống

Bước 2: Chọn 

để lưu thông tin HTTT vừa nhập

Cập nhật hệ thống thông tin

Mục đích: Chức năng này giúp người dùng cập nhật thông tin hồ sơ đề xuất cấp độ của HTTT

Thao tác:

Bước 1: Từ danh sách HTTT di chuột sang tay phải màn hình chọn  để cập nhật thông tin về HTTT, hệ thống sẽ điều hướng sang màn hình xây dựng hồ sơ đề xuất cấp độ để người dùng tiến hành cập nhật

Hình 16: Màn hình cập nhật hệ thống thông tin

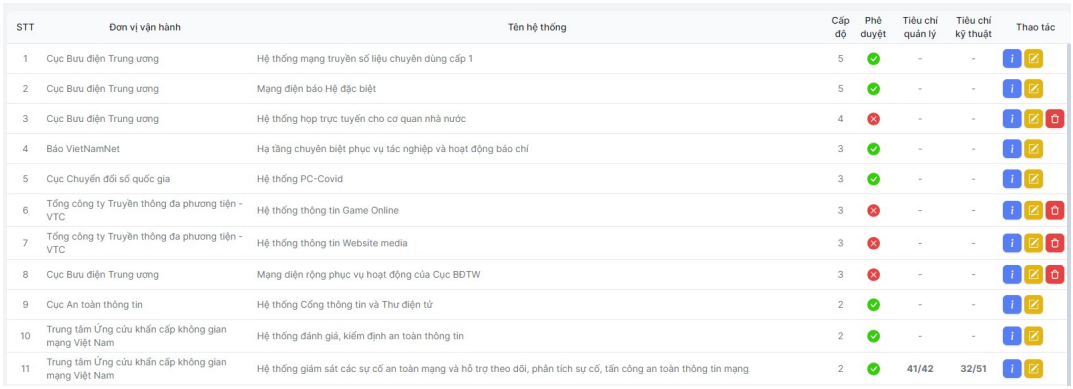
Bước 2: Chọn tạo mới hoặc sử dụng hồ sơ mẫu đã có để bắt đầu xây dựng hồ sơ đề xuất cấp độ

Chi tiết hệ thống thông tin

Mục đích: Chức năng này giúp người dùng xem danh sách HTTT đã duyệt trong đơn vị, tìm kiếm HTTT theo tên hoặc theo cấp độ HTTT

Thao tác:

Bước 1: Từ danh sách HTTT, click chọn vào nút  của dòng HTTT để xem chi tiết thông tin về HTTT



STT	Đơn vị vận hành	Tên hệ thống	Cấp độ	Phê duyệt	Tiêu chí quản lý	Tiêu chí kỹ thuật	Thao tác
1	Cục Bưu điện Trung ương	Hệ thống mạng truyền số liệu chuyên dùng cấp 1	5	✓	-	-	
2	Cục Bưu điện Trung ương	Mạng điện báo Hệ đặc biệt	5	✓	-	-	
3	Cục Bưu điện Trung ương	Hệ thống họp trực tuyến cho cơ quan nhà nước	4	✗	-	-	
4	Báo VietNamNet	Hạ tầng chuyên biệt phục vụ tác nghiệp và hoạt động báo chí	3	✓	-	-	
5	Cục Chuyển đổi số quốc gia	Hệ thống PC-Covid	3	✓	-	-	
6	Tổng công ty Truyền thông đa phương tiện - VTC	Hệ thống thông tin Game Online	3	✗	-	-	
7	Tổng công ty Truyền thông đa phương tiện - VTC	Hệ thống thông tin Website media	3	✗	-	-	
8	Cục Bưu điện Trung ương	Mạng điện rộng phục vụ hoạt động của Cục BĐTW	3	✗	-	-	
9	Cục An toàn thông tin	Hệ thống Cổng thông tin và Thư điện tử	2	✓	-	-	
10	Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam	Hệ thống đánh giá, kiểm định an toàn thông tin	2	✓	-	-	
11	Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam	Hệ thống giám sát các sự cố an toàn mạng và hỗ trợ theo dõi, phân tích sự cố, tấn công an toàn thông tin mạng	2	✓	41/42	32/51	

Hình 17: Màn danh sách hệ thống thông tin

Bước 2: Màn thông tin chi tiết HTTT, người dùng có thể xem thông tin và cập nhật các tài liệu liên quan của HTTT

Hình 18: Màn chi tiết hệ thống thông tin

d) Hồ sơ đề xuất cấp độ

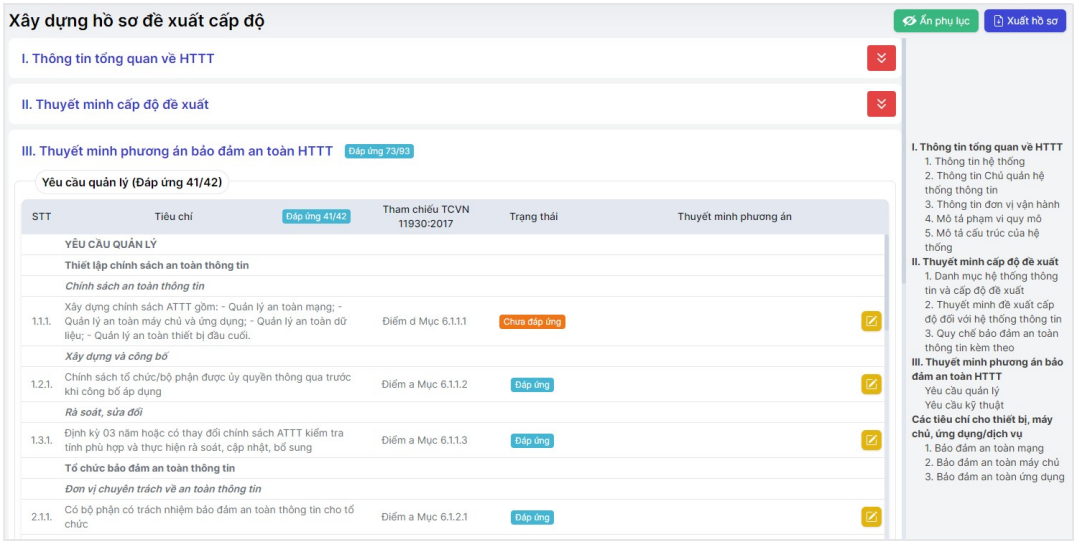
Xây dựng HSĐXCĐ cho HTTT

<u>Mục đích:</u> Chức năng này giúp người dùng xây dựng hồ sơ đề xuất các cấp độ trong HTTT

<u>Thao tác</u>:

Bước 1: Từ màn danh sách HTTT chọn  để chuyển đến màn "Xây dựng hồ sơ đề xuất cấp độ"

Bước 2 : Màn "Xây dựng sơ đề xuất cấp độ" hiển thị



Hình 19: Màn xây dựng dự thảo hồ sơ đề xuất cấp độ

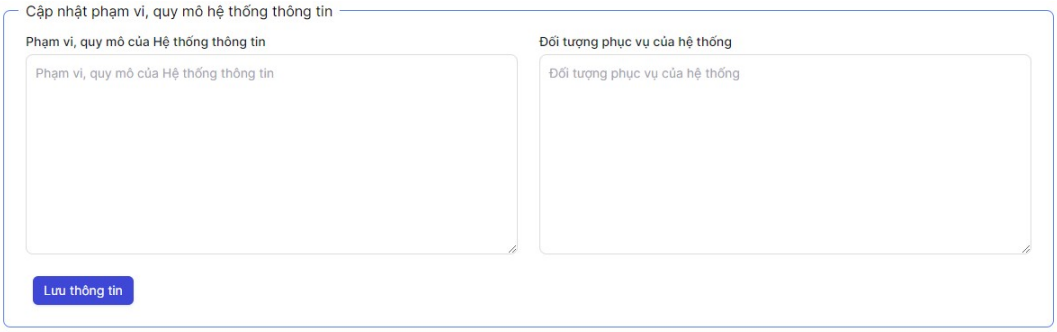
Người dùng thao tác nhấn nút » hoặc click các mục trên phụ lục để cập nhật thông tin của HTTT

Mô tả phạm vi quy mô

Mục đích: Cập nhật phạm vi, quy mô của HTTT

Thao tác:

Bước 1: Từ màn hình HSĐXCĐ, tại mục 4. Mô tả phạm vi quy mô chọn Cập nhật thông tin



Hình 20: Màn phạm vi, quy mô HTTT hồ sơ đề xuất cấp độ

Bước 2: Nhập thông tin và chọn Lưu thông tin

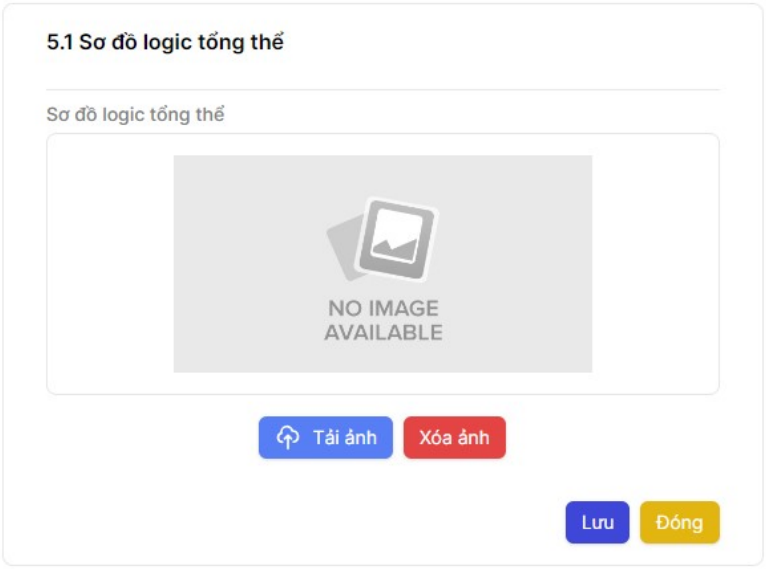
Mô tả cấu trúc của hệ thống

Mục đích: Chức năng này giúp người dùng cập nhật các sơ đồ logic và sơ đồ kết nối vật lý của HTTT

Thao tác:

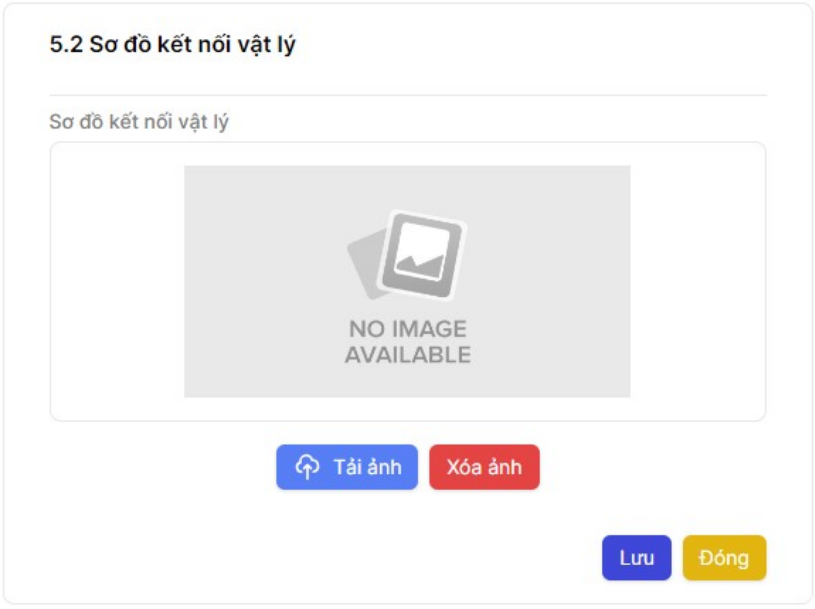
Bước 1: Từ màn hình HSĐXCĐ, tại mục 4. Mô tả phạm vi quy mô chọn Cập nhật từng sơ đồ của hệ thống

Bước 2: Tải ảnh sơ đồ logic tổng thể của hệ thống và nhấn lưu



Hình 21: Màn hình sơ đồ logic tổng thể

Bước 3: Tải ảnh sơ đồ kết nối vật lý của hệ thống và nhấn lưu



Hình 22: Màn hình sơ đồ kết nối vật lý

Thiết kế các vùng mạng

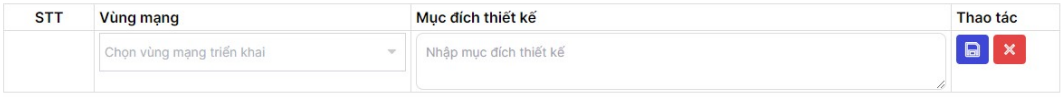
Mục đích: Chức năng này giúp người dùng cập nhật danh sách các vùng mạng trong HTTT

Thao tác:

Bước 1: Từ màn hình HSĐXCĐ, tại mục 5.3 Thiết kế các vùng mạng, chọn Thêm vùng mạng

Hình 23: Màn danh sách vùng mạng trong HTTT

Bước 2: Chọn vùng mạng sử dụng và nhập mục đích sử dụng



Hình 24: Màn thêm vùng mạng trong HTTT

- **"Vùng mạng"**: Chọn vùng mạng mới
- **"Mục đích thiết kế":** Nhập thông tin mục đích

Bước 3: Chọn để lưu thông tin thiết bị vừa nhập

Bước 4: Người dùng cũng có thể chọn để sửa thông tin thiết bị, hoặc chọn để xóa thiết bị khỏi danh sách

Danh mục thiết bị mạng/bảo mật sử dụng trong hệ thống

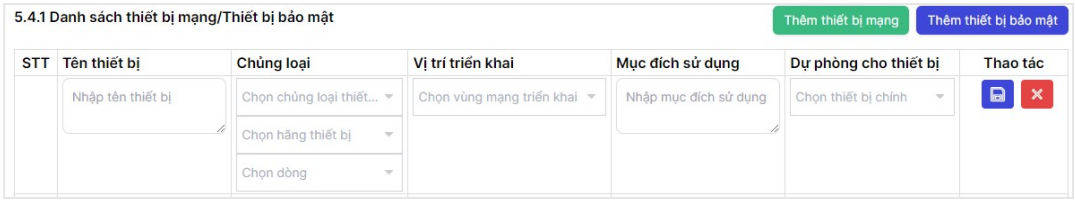
Mục đích: Chức năng này giúp người dùng cập nhật danh sách các thiết bị trong HTTT

Thao tác:

Bước 1: Từ màn hình HSĐXCĐ, tại mục 5.4.1 Danh mục thiết bị mạng/bảo mật sử dụng trong hệ thống hiển thị danh sách thiết bị mạng, thiết bị bảo mật được sử dụng trong HTTT

Hình 25: Màn danh sách thiết bị mạng, bảo mật trong HTTT

Bước 2: Người dùng có thể chọn thêm mới hoặc cập nhật các thiết bị trong HTTT



Hình 26: Màn thêm mới thiết bị trong HTTT

- **"Tên thiết bị"**: Nhập tên của thiết bị
- **"Chủng loại"**: Chọn chủng loại thiết bị
- **"Hãng thiết bị"**: Chọn hãng thiết bị
- **"Model"**: Chọn dòng thiết bị theo hãng
- **"Vị trí triển khai"**: Nhập vị trí đặt thiết bị
- **"Mục đích sử dụng"**: Mục đích sử dụng của thiết bị
- **"Dự phòng cho thiết bị"**: Chọn thiết bị chính cần dự phòng(Nếu đang nhập thiết bị dự phòng)

Bước 3: Chọn để lưu thông tin thiết bị vừa nhập

Bước 4: Người dùng cũng có thể chọn để sửa thông tin thiết bị, hoặc chọn để xóa thiết bị khỏi danh sách

Danh mục thiết bị máy chủ trong hệ thống

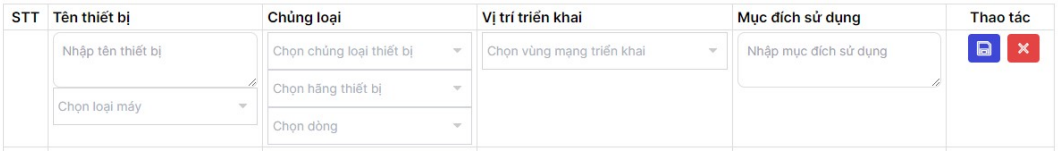
Mục đích: Chức năng này giúp người dùng cập nhật danh sách các thiết bị máy chủ trong HTTT

Thao tác:

Bước 1: Từ màn hình HSĐXCĐ, tại mục 5.4.2 Danh mục thiết bị máy chủ sử dụng trong hệ thống hiển thị danh sách thiết máy chủ được sử dụng trong HTTT

Hình 27: Màn danh sách thiết bị máy chủ trong HTTT

Bước 2: Người dùng có thể chọn thêm mới hoặc cập nhật các thiết bị trong HTTT



Hình 28: Màn thêm mới thiết bị máy chủ trong HTTT

- **"Tên thiết bị"**: Nhập tên của thiết bị
- **"Loại máy"**: Chọn loại máy vật lý hoặc máy chủ ảo hóa
- **"Chủng loại"**: Chọn chủng loại thiết bị
- **"Hãng thiết bị"**: Chọn hãng thiết bị
- **"Model"**: Chọn dòng thiết bị theo hãng
- **"Vị trí triển khai"**: Nhập vị trí đặt thiết bị
- **"Mục đích sử dụng"**: Mục đích sử dụng của thiết bị

Bước 3: Chọn để lưu thông tin thiết bị vừa nhập

Bước 4: Người dùng cũng có thể chọn để sửa thông tin thiết bị, hoặc chọn để xóa thiết bị khỏi danh sách

Danh sách dịch vụ

Mục đích: Chức năng này giúp người dùng cập nhật danh sách các dịch vụ trong HTTT

Thao tác:

Bước 1: Từ màn hình HSĐXCĐ, tại mục 5.5 Danh mục các ứng dụng/dịch vụ cung cấp bởi hệ thống hiển thị danh sách ứng dụng cài đặt trên máy chủ trong HTTT

Bước 2: Danh sách dịch vụ hiển thị các dịch vụ, ứng dụng được sử dụng trong HTTT

Hình 29: Màn danh sách dịch vụ thuộc HTTT

Bước 3: Người dùng có thể thêm mới các dịch vụ vào HTTT

Hình 30: Màn thêm mới dịch vụ thuộc HTTT

- **"Tên dịch vụ"**: Nhập tên dịch vụ
- **"Máy chủ"**: Chọn loại máy chủ
- **"Ứng dụng cài đặt"**: Nhập tên ứng dụng cài đặt
- **"Vùng mạng"**: Chọn vùng mạng
- **"Hệ điều hành"**: Nhập tên hệ diều hành
- **"Mục đích sử dụng"**: Nhập mục đích sử dụng

Bước 4 : Chọn để lưu thông tin thiết bị vừa nhập

Bước 5: Người dùng cũng có thể chọn để sửa thông tin thiết bị, hoặc chọn để xóa dịch vụ khỏi danh sách

Danh sách IP vùng mạng

Mục đích: Chức năng này giúp người dùng xem danh sách IP vùng mạng, tìm kiếm HTTT theo tên hoặc theo cấp độ HTTT

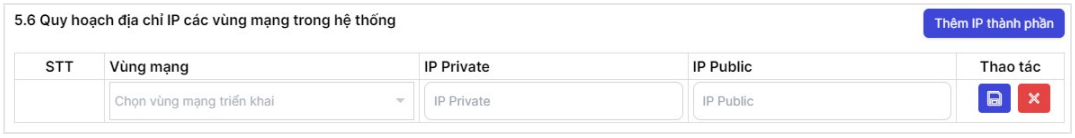
Thao tác:

Bước 1: Từ màn hình HSĐXCĐ, tại mục 5.6 Quy hoạch địa chỉ IP các vùng mạng trong hệ thống

Bước 2: Danh sách IP vùng mạng hiển thị các IP được sử dụng trong HTTT

Hình 31: Màn danh sách IP thuộc HTTT

Bước 3: Người dùng có thể chọn Thêm IP thành phần để mới IP của HTTT



Hình 32: Màn thêm mới địa chỉ IP

- **"Vị trí triển khai"**: Nhập vị trí đặt thiết bị
- **"IP Public"**: IP công khai
- **"IP Private"**: IP bảo mật

Bước 4: Chọn nút Lưu lại để lưu lại danh sách thông tin IP đã cập nhật

Danh mục máy trạm trong HTTT

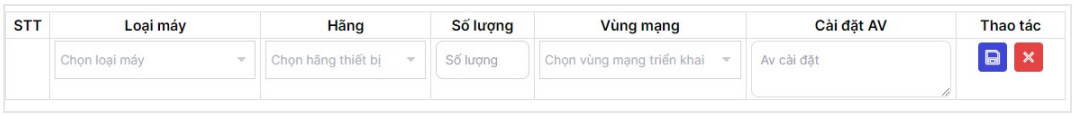
Mục đích: Chức năng này giúp người dùng cập nhật danh sách các thiết bị máy trạm trong HTTT

Thao tác:

Bước 1: Từ màn hình HSĐXCĐ, tại mục 5.4.2 Danh mục thiết bị máy chủ sử dụng trong hệ thống hiển thị danh sách thiết máy chủ được sử dụng trong HTTT

Hình 33: Màn danh sách thiết bị máy trạm trong HTTT

Bước 2: Người dùng có thể chọn thêm mới hoặc cập nhật các thiết bị trong HTTT



Hình 34: Màn thêm mới thiết bị trong HTTT

- **"Loại máy"**: Chọn loại máy PC hoặc máy laptop
- **"Hãng thiết bị"**: Chọn hãng thiết bị
- **"Số lượng"**: Chọn số lượng thiết bị theo hãng
- **"Vùng mạng"**: Nhập vùng mạng sử dụng
- **"Cài đặt AV"**: Thông tin phần mềm AV cài đặt trên máy

Bước 3: Chọn để lưu thông tin thiết bị vừa nhập

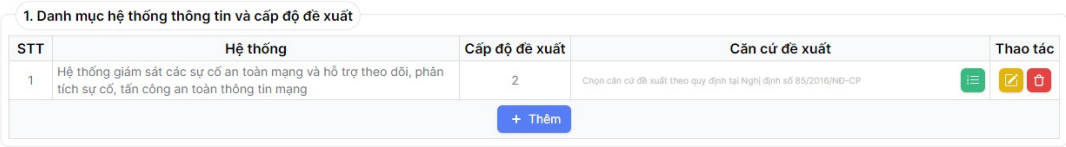
Bước 4: Người dùng cũng có thể chọn để sửa thông tin thiết bị, hoặc chọn để xóa thiết bị khỏi danh sách

Danh mục hệ thống thông tin và cấp độ đề xuất

Mục đích: Chức năng này giúp người dùng cập nhật danh sách các hệ thống thành phần trong HTTT

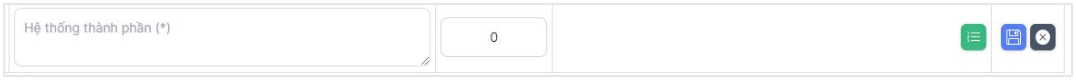
Thao tác:

Bước 1: Từ màn hình HSĐXCĐ, tại phần II mục 1 Danh mục hệ thống thông tin và cấp độ đề xuất hiển thị danh sách hệ thống thành phần trong HTTT

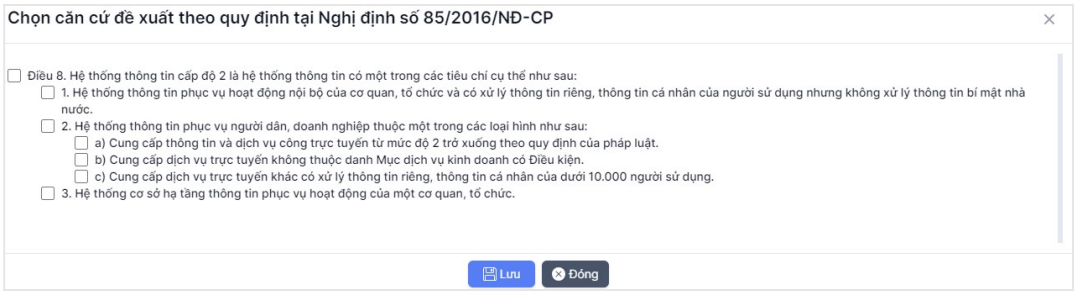


Hình 35: Màn danh sách hệ thống thành phần trong HTTT

Bước 2: Người dùng có thể chọn thêm mới hoặc cập nhật các hệ thống thành phần trong HTTT



Hình 36: Màn thêm mới hệ thống thành phần trong HTTT



Hình 37: Màn chọn căn cứ đề xuất theo cấp độ của HTTT

- **"Hệ thống thành phần"**: Nhập tên hệ thống thành phần
- **"Cấp độ đề xuất"**: Chọn cấp độ của hệ thống thành phần
- **"Căn cứ đề xuất"**: Chọn các căn cứ đề xuất

Bước 3: Chọn  để lưu thông tin thiết bị vừa nhập

Bước 4: Người dùng cũng có thể chọn  để sửa thông tin thiết bị, hoặc chọn  để xóa thiết bị khỏi danh sách

Thuyết minh đề xuất cấp độ đối với hệ thống thông tin

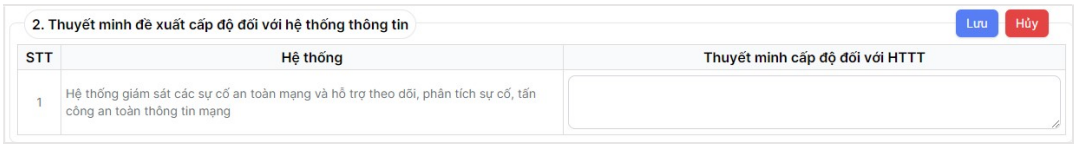
Mục đích: Chức năng này giúp người dùng cập nhật danh sách các thuyết minh đề xuất cấp độ các hệ thống trong HTTT

Thao tác:

Bước 1: Từ màn hình HSĐXCĐ, tại phần II mục 2 Thuyết minh đề xuất cấp độ đối với HTTT hiển thị danh sách thuyết minh hệ thống thành phần trong HTTT

Hình 38: Màn danh sách thuyết minh hệ thống thành phần trong HTTT

Bước 2: Người dùng có thể cập nhật các thuyết minh hệ thống thành phần trong HTTT



Hình 39: Màn cập nhật thuyết minh hệ thống thành phần trong HTTT

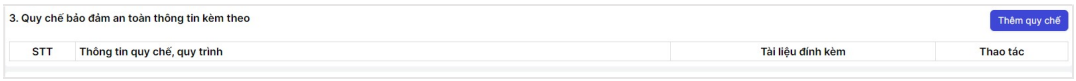
Bước 3: Chọn Lưu để lưu thông tin thiết bị vừa nhập

Quy chế bảo đảm an toàn thông tin kèm theo

Mục đích: Chức năng này giúp người dùng cập nhật danh sách các quy chế trong HTTT

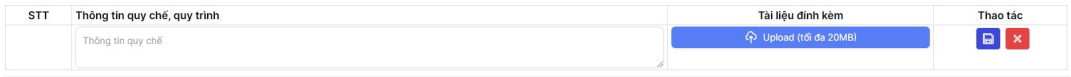
Thao tác:

Bước 1: Từ màn hình HSĐXCĐ, tại phần II mục 3 Danh mục quy chế đảm bảo ATTT trong HTTT



Hình 40: Màn danh sách quy chế trong HTTT

Bước 2: Người dùng có thể chọn thêm mới hoặc cập nhật các quy chế trong HTTT



Hình 41: Màn thêm mới quy chế trong HTTT

- **"Thông tin quy chế"**: Nhập tên thông tin quy chế hệ thống thông tin
- **"Tài liệu đính kèm"**: upload tài liệu liên quan

Bước 3: Chọn để lưu thông tin vừa nhập

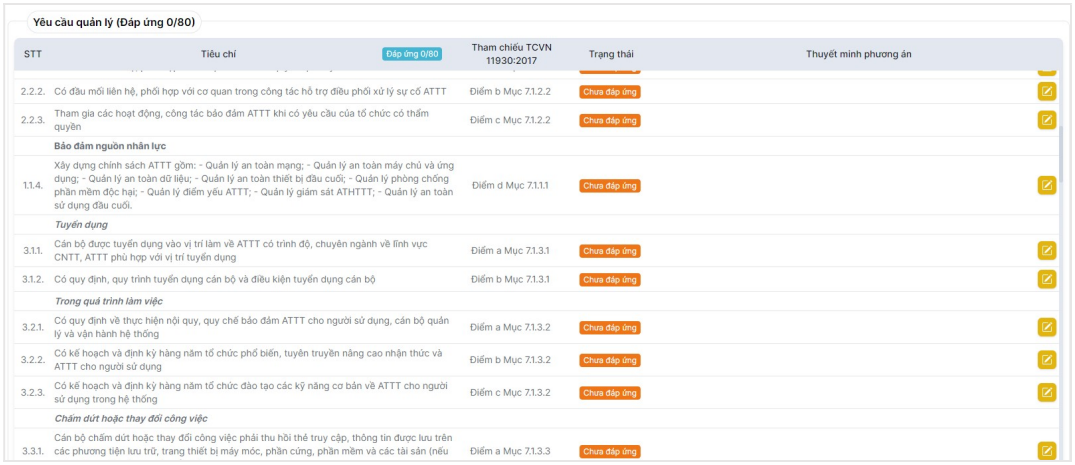
Bước 4: Người dùng cũng có thể chọn để sửa thông tin, hoặc chọn để xóa tài liệu khỏi danh sách

Phương án bảo đảm an toàn HTTT - Yêu cầu quản lý

Mục đích: Người dùng cập nhật lại thông tin thuyết minh các phương án đảm bảo ATHTTT

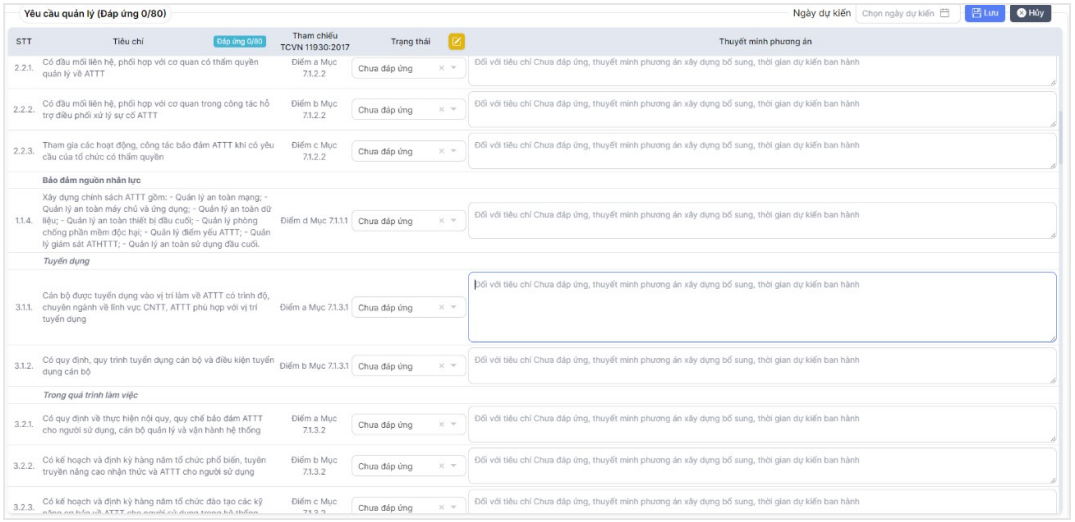
Thao tác:

Bước 1: Từ màn hình HSĐXCĐ, tại phần III. Thuyết minh phương án bảo đảm an toàn HTTT, hiển thị mục Yêu cầu quản lý



Hình 42: Màn danh sách Yêu cầu quản lý Phương án đảm bảo an toàn HTTT

Bước 2: Người dùng có thể cập nhật từng tiêu chí đáp ứng của HTTT



Hình 43: Màn cập nhật Phương án triển khai

- **"Trạng thái "**: Chọn trạng thái đáp ứng tiêu chí
- **"Ngày dự kiến"**: Nếu chưa đáp ứng, chọn thời gian dự kiến
- **"Phương án"**: Ghi chú về thông tin phương án

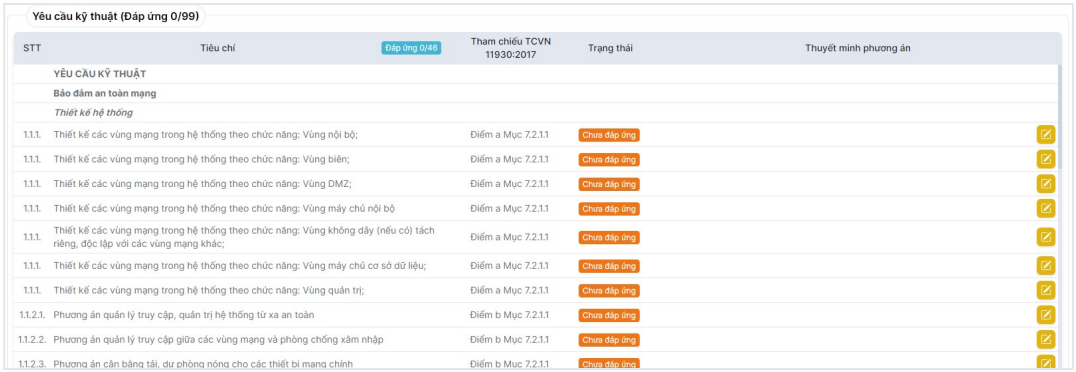
Bước 3: Chọn nút Lưu để lưu lại danh sách thông tin tiêu chí đã cập nhật

Phương án bảo đảm an toàn HTTT - Yêu cầu quản lý

<u>Mục đích:</u> Người dùng cập nhật lại thông tin thuyết minh các phương án đảm bảo ATHTTT

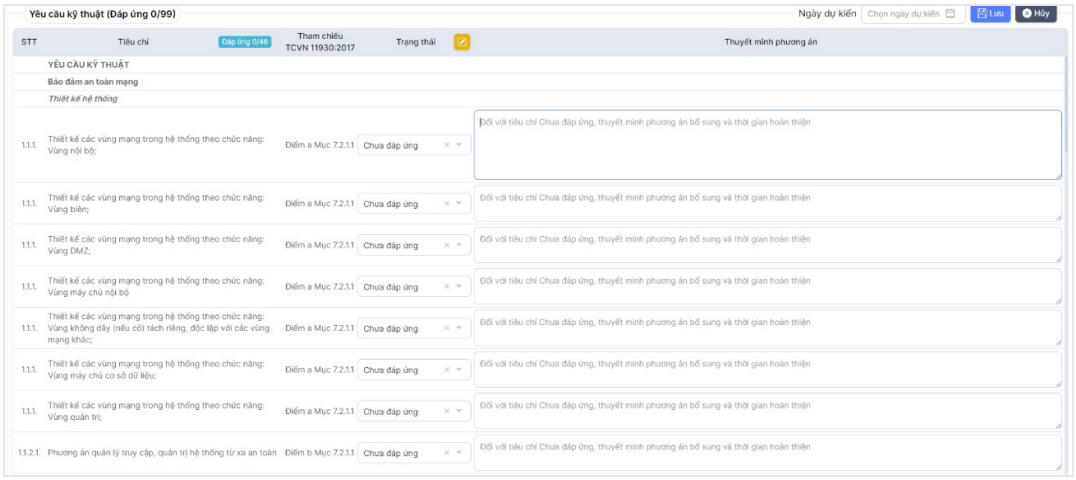
<u>Thao tác:</u>

Bước 1: Từ màn hình HSĐXCĐ, tại phần III. Thuyết minh phương án bảo đảm an toàn HTTT, hiển thị mục Yêu cầu kỹ thuật



Hình 44: Màn danh sách Yêu cầu kỹ thuật Phương án đảm bảo an toàn HTTT

Bước 2: Người dùng có thể cập nhật từng tiêu chí đáp ứng của HTTT



Hình 45: Màn cập nhật Phương án triển khai

- **"Trạng thái "**: Chọn trạng thái đáp ứng tiêu chí
- **"Ngày dự kiến"**: Nếu chưa đáp ứng, chọn thời gian dự kiến
- **"Phương án"**: Ghi chú về thông tin phương án

Bước 3: Chọn nút 

để lưu lại danh sách thông tin tiêu chí đã cập nhật

e) Cấu hình

Đơn vị vận hành

<u>Mục đích:</u> Hiển thị danh sách đơn vị vận hành HTTT của đơn vị

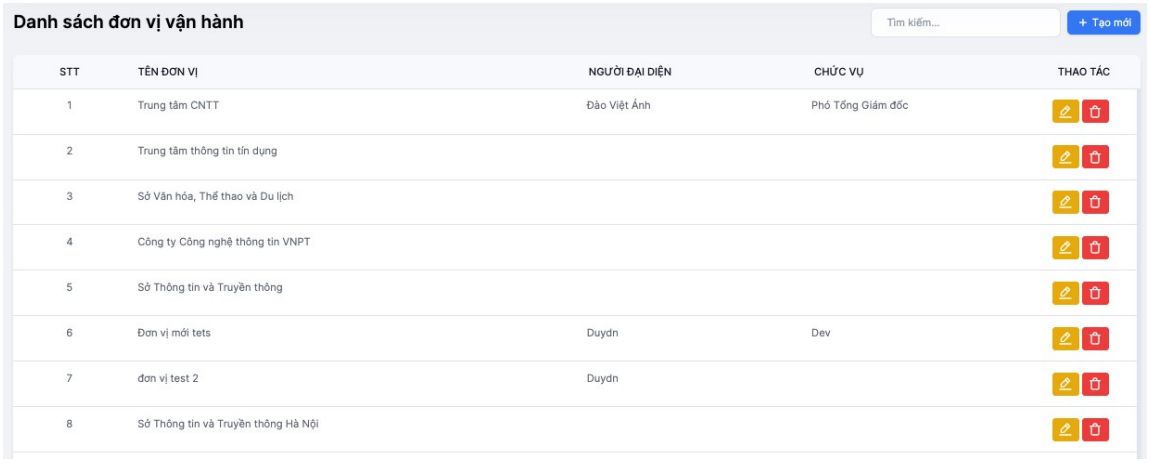
Tại màn danh sách đơn vị vận hành người dùng có thể tìm kiếm theo tên chọn

<u>Thao tác</u>:

Bước 1: Từ menu trái chọn 

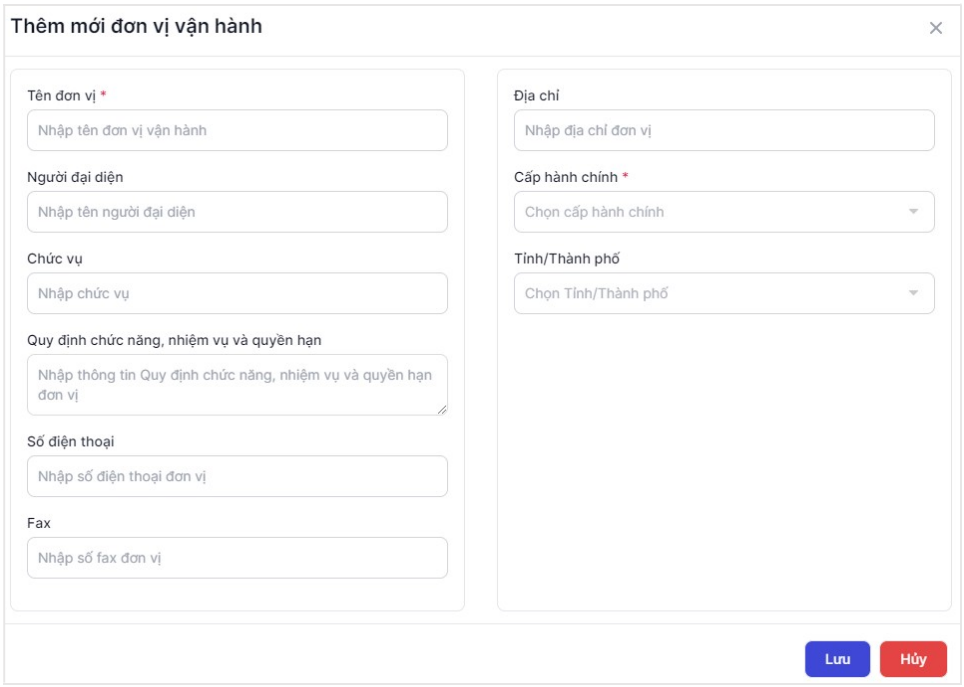
để chuyển đến màn "**Danh sách đơn vị vận hành**"

Bước 2: Màn "**Danh sách đơn vị vận hành**" hiển thị danh sách đơn vị vận hành HTTT của đơn vị



Hình 46: Màn danh sách đơn vị vận hành

Bước 3: Người dùng đơn vị có thể thêm mới thông tin đơn vị vận hành bằng cách di chuyển chuột sang tay phải màn hình chọn cập nhật thông tin đơn vị



Hình 47: Màn thêm mới đơn vị vận hành

- "Tên đơn vị": Nhập tên đơn vị vận hành

- "Người đại diện": Người đại diện đơn vị

- "Chức vụ": Chức vụ người đại diện

- **"Quy định": Quy định đơn vị**
- **"Chức năng": Chức năng của đơn vị vận hành**
- **"Nhiệm vụ": Nhiệm vụ của đơn vị vận hành**
- **"Số điện thoại": Nhập số điện thoại**
- **"Fax": Nhập số fax**
- **"Địa chỉ": Nhập địa chỉ đơn vị vận hành**
- **"Cấp hành chính": Chọn cấp cơ quan của đơn vị vận hành**

Bước 4: Nhập các thông tin chỉnh sửa và chọn Lưu để lưu thông tin

Tài khoản đơn vị vận hành

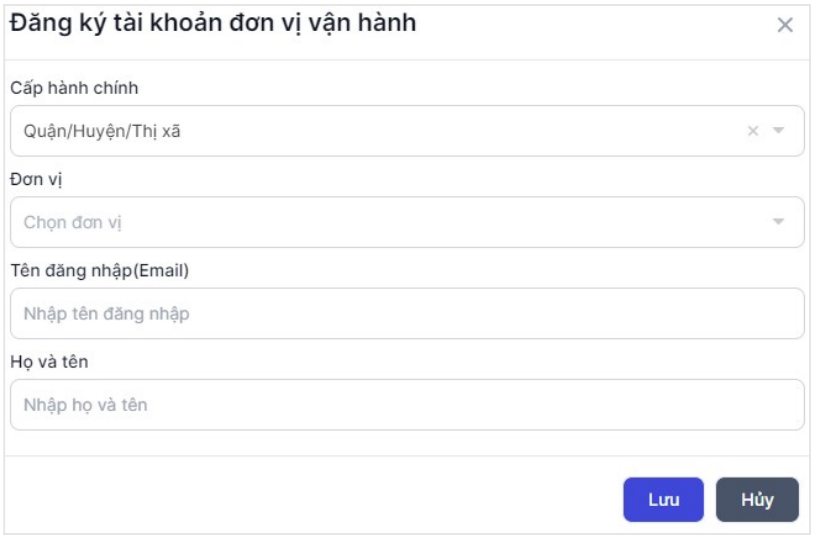
Mục đích: Hiển thị danh sách các tài khoản của đơn vị vận hành thuộc cơ quan chủ quản

Thao tác:

Bước 1: Từ menu trái chọn Tài khoản đơn vị vận hành để chuyển đến màn "**Danh sách tài khoản đơn vị vận hành"**

Bước 2: Người dùng đơn vị chuyên trách có thể tra cứu thông tin, thêm mới, cập nhật thông tin tài khoản các đơn vị vận hành trực thuộc.

Bước 3: Để thêm mới "Tài khoản", người dùng chọn + Tạo mới ở phía bên phải.



Hình 48: Màn đăng ký tài khoản đơn vị vận hành

- **"Cấp hành chính":** Chọn cấp cơ quan đơn vị vận hành
- **"Đơn vị":** Chọn đơn vị vận hành theo cấp hành chính
- **"Tên đăng nhập(Email)":** Nhập email của đơn vị vận hành
- **"Họ tên" :** Nhập tên đơn vị vận hành

Bước 4: Chọn Lưu **để lưu thông tin**

f) Tài liệu - Hỏi đáp

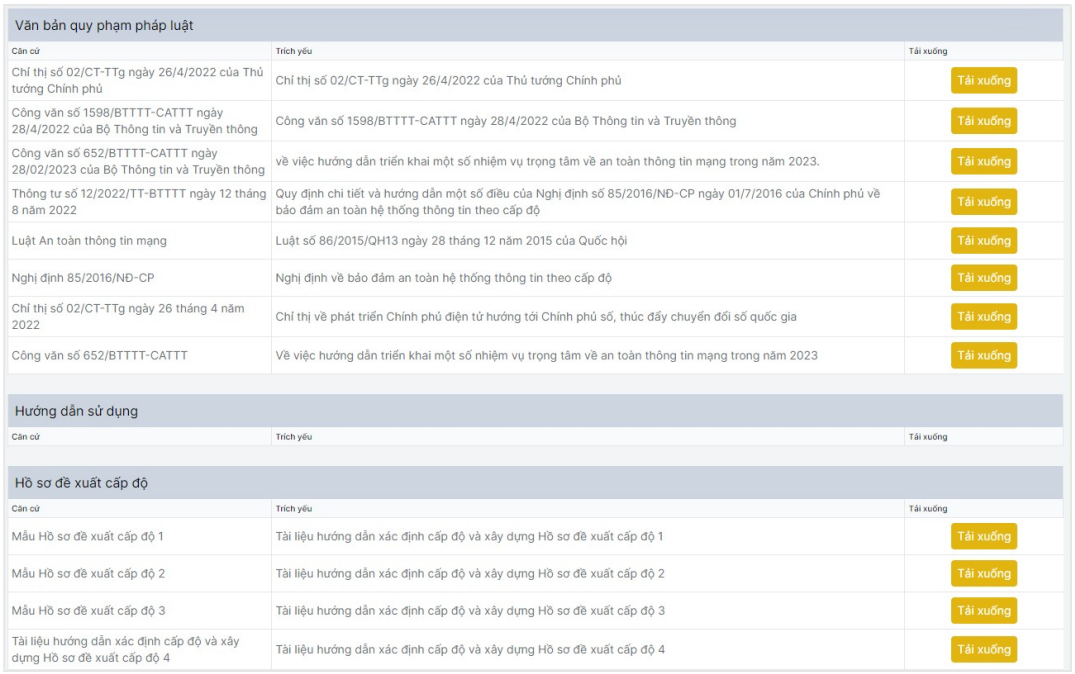
Tài liệu

Mục đích: Hiển thị danh sách tài liệu quy phạm pháp luật, tài liệu hướng dẫn

Thao tác:

Bước 1: Từ menu trái chọn Tài liệu để chuyển đến màn "**Tài liệu**"

Bước 2: Màn "**Tài liệu**" hiển thị danh sách các tài liệu liên quan, được chia thành các nhóm: Văn bản quy phạm pháp luật, Hướng dẫn sử dụng, Hồ sơ đề xuất cấp độ, Biểu mẫu công văn



Văn bản quy phạm pháp luật

Căn cứ	Trích yếu	Tải xuống
Chỉ thị số 02/CT-TTg ngày 26/4/2022 của Thủ tướng Chính phủ	Chỉ thị số 02/CT-TTg ngày 26/4/2022 của Thủ tướng Chính phủ	Tải xuống
Công văn số 1598/BTTTT-CATTT ngày 28/4/2022 của Bộ Thông tin và Truyền thông	Công văn số 1598/BTTTT-CATTT ngày 28/4/2022 của Bộ Thông tin và Truyền thông	Tải xuống
Công văn số 652/BTTTT-CATTT ngày 28/02/2023 của Bộ Thông tin và Truyền thông	về việc hướng dẫn triển khai một số nhiệm vụ trọng tâm về an toàn thông tin mạng trong năm 2023.	Tải xuống
Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022	Quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ	Tải xuống
Luật An toàn thông tin mạng	Luật số 86/2015/QH13 ngày 28 tháng 12 năm 2015 của Quốc hội	Tải xuống
Nghị định 85/2016/NĐ-CP	Nghị định về bảo đảm an toàn hệ thống thông tin theo cấp độ	Tải xuống
Chỉ thị số 02/CT-TTg ngày 26 tháng 4 năm 2022	Chỉ thị về phát triển Chính phủ điện tử hướng tới Chính phủ số, thúc đẩy chuyển đổi số quốc gia	Tải xuống
Công văn số 652/BTTTT-CATTT	Về việc hướng dẫn triển khai một số nhiệm vụ trọng tâm về an toàn thông tin mạng trong năm 2023	Tải xuống

Hướng dẫn sử dụng

Căn cứ	Trích yếu	Tải xuống

Hồ sơ đề xuất cấp độ

Căn cứ	Trích yếu	Tải xuống
Mẫu Hồ sơ đề xuất cấp độ 1	Tài liệu hướng dẫn xác định cấp độ và xây dựng Hồ sơ đề xuất cấp độ 1	Tải xuống
Mẫu Hồ sơ đề xuất cấp độ 2	Tài liệu hướng dẫn xác định cấp độ và xây dựng Hồ sơ đề xuất cấp độ 2	Tải xuống
Mẫu Hồ sơ đề xuất cấp độ 3	Tài liệu hướng dẫn xác định cấp độ và xây dựng Hồ sơ đề xuất cấp độ 3	Tải xuống
Tài liệu hướng dẫn xác định cấp độ và xây dựng Hồ sơ đề xuất cấp độ 4	Tài liệu hướng dẫn xác định cấp độ và xây dựng Hồ sơ đề xuất cấp độ 4	Tải xuống

Hình 49: Màn danh tài liệu công văn

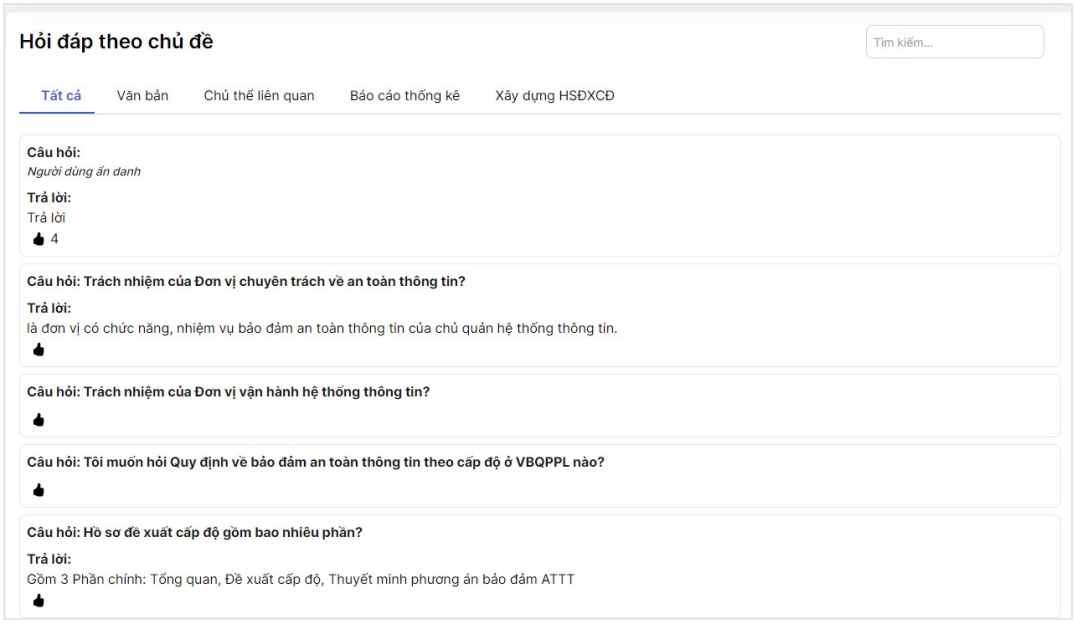
Bước 3: Người dùng đơn vị có thể tải các tài liệu để tham khảo

Hỏi đáp

Mục đích: Hiển thị danh sách các câu hỏi về các chủ đề liên quan trong hệ thống

Thao tác:

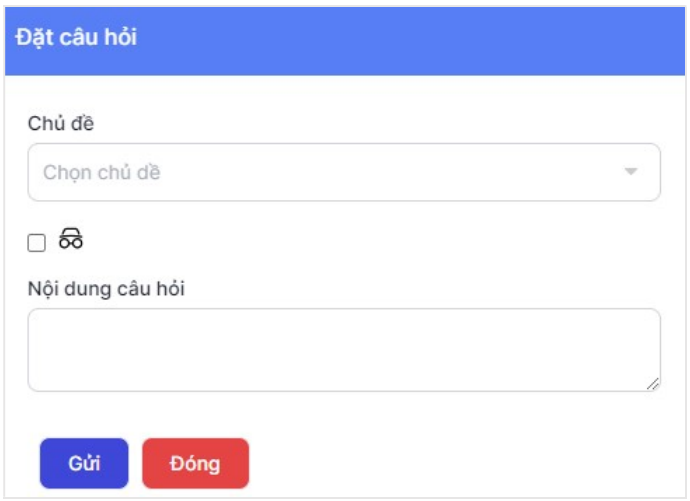
Bước 1: Từ menu trái chọn Hỏi đáp để chuyển đến màn "**Hỏi đáp theo chủ đề**"



Hình 50: Màn danh sách câu hỏi theo chủ đề

Bước 2: Người dùng đơn vị có thể lọc câu hỏi theo chủ đề hoặc tìm kiếm theo từ khóa

Bước 3: Để thêm mới "Tài khoản", người dùng chọn + Tạo mới ở phía bên phải.



Hình 51: Màn đăng ký câu hỏi

g) **"Chủ đề"**: Chọn chủ đề cần hỏi

h) **"Ẩn danh"**: Chọn nếu muốn hỏi ẩn danh

i) **"Nội dung câu hỏi" :** Nhập vấn đề cần hỏi

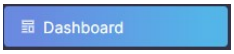
Bước 4: Chọn Gửi để gửi thông tin câu hỏi lên hệ thống

2.2. Đối với tài khoản Đơn vị vận hành

a) Chức năng Thống kê

Mục đích: Để người dùng có thể nắm bắt được thông tin số liệu , tỷ lệ phê duyệt HTTT qua những biểu đồ thống kê.

Thao tác:

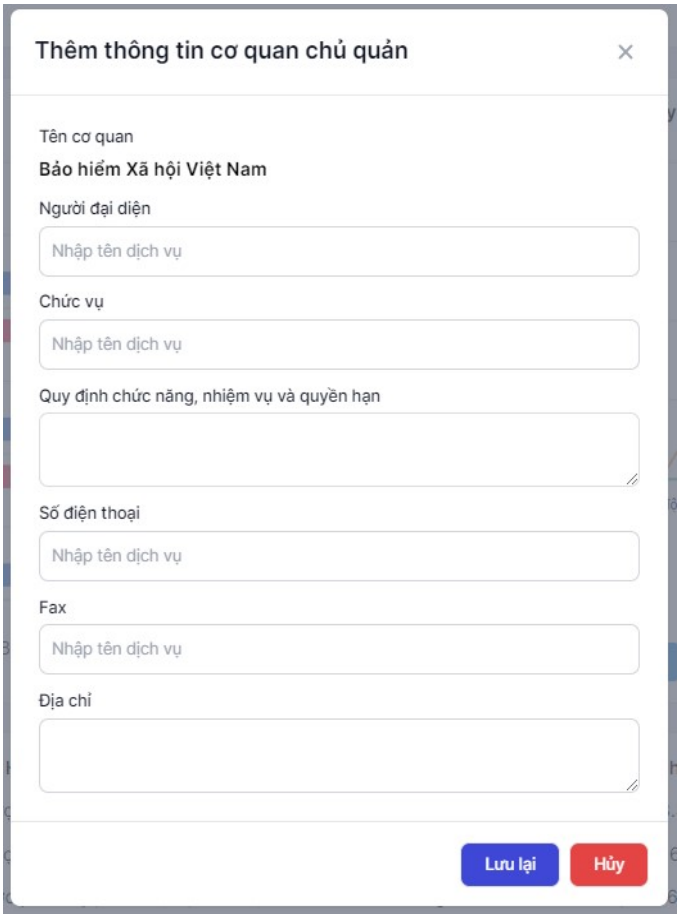
Bước 1: Từ menu trái chọn 

để chuyển đến màn "**Biểu đồ thống kê HTTT**"

Bước 2: Màn "**Biểu đồ thống kê HTTT**" hiển thị thống kê tỷ lệ phê duyệt , số liệu phê duyệt HTTT với cả nước

Hình 4: Màn biểu đồ thống kê số liệu HTTT

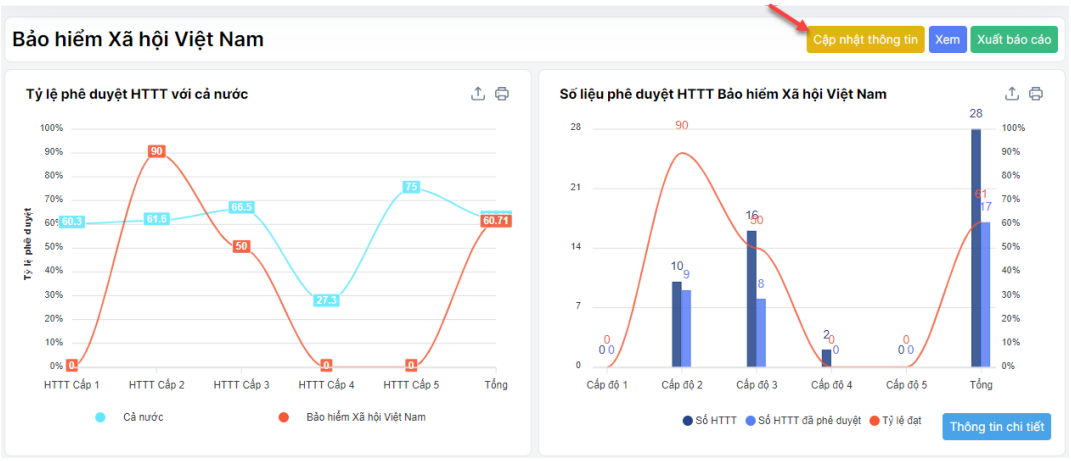
Bước 3: Có thể Thêm thông tin cơ quan chủ quản



Hình 5: Màn nhập thông tin đơn vị chủ quản

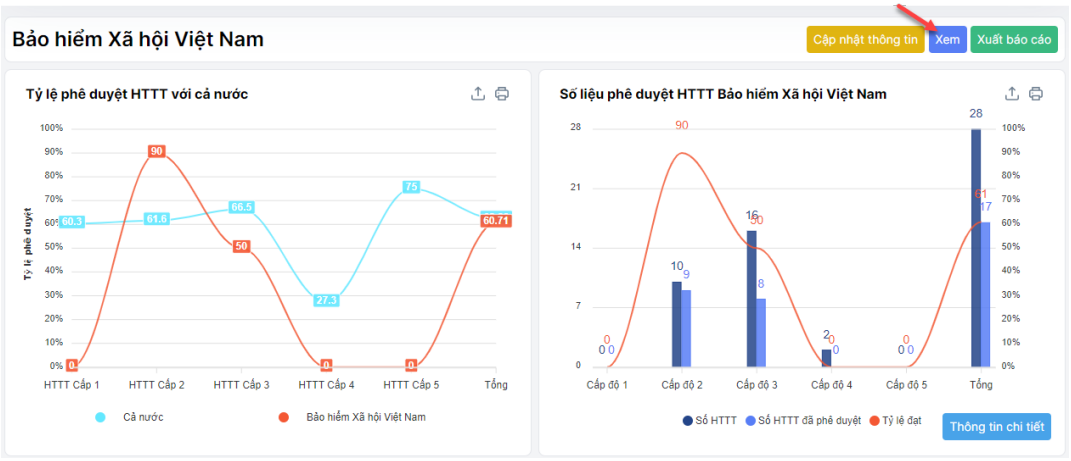
Điền thông tin đầy đủ xong chọn lưu lại để lưu thông tin vừa nhập

Bước 4: Sau khi nhập xong thông tin người dùng có thể cập nhật bằng cách chọn: "Cập nhật thông tin"



Hình 6: Màn biểu đồ thống kê số liệu HTTT

Hoặc xem thông tin

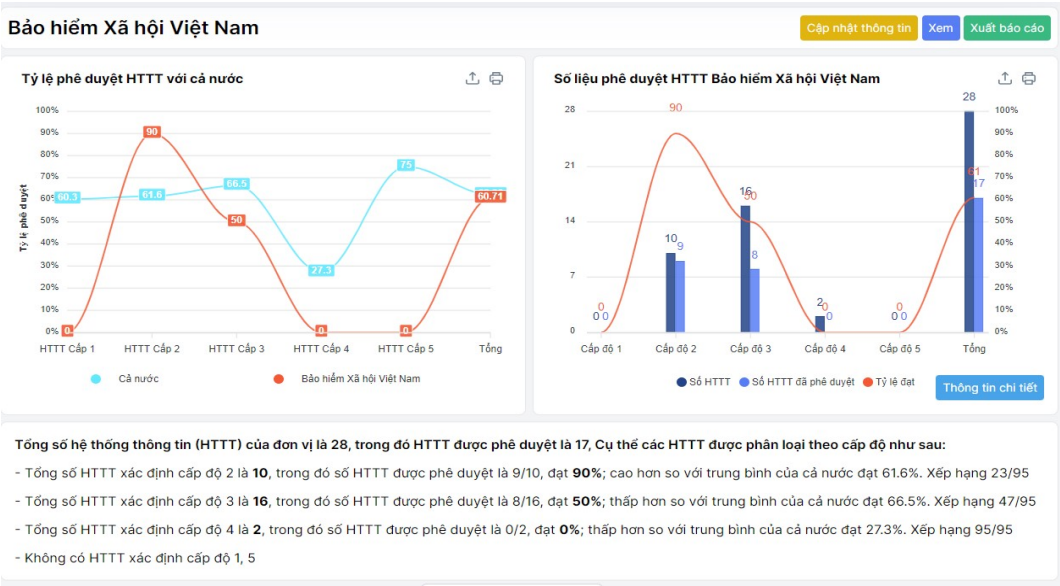


Hình 7: Màn biểu đồ thống kê số liệu HTTT

Người dùng cũng có thể xuất thông tin bằng cách Xuất báo cáo

Hình 8: Màn biểu đồ thống kê số liệu HTTT

Bước 5: Chọn Thông tin chi tiết thông tin chi tiết số liệu phê duyệt HTTT sẽ được hiển thị đầy đủ bên dưới



Hình 9: Màn biểu đồ thống kê số liệu HTTT

b) Chức năng Báo cáo, thống kê

Chức năng cho phép người dùng tạo mới, gửi và quản lý danh sách các số liệu hệ thống thông tin đã thống kê

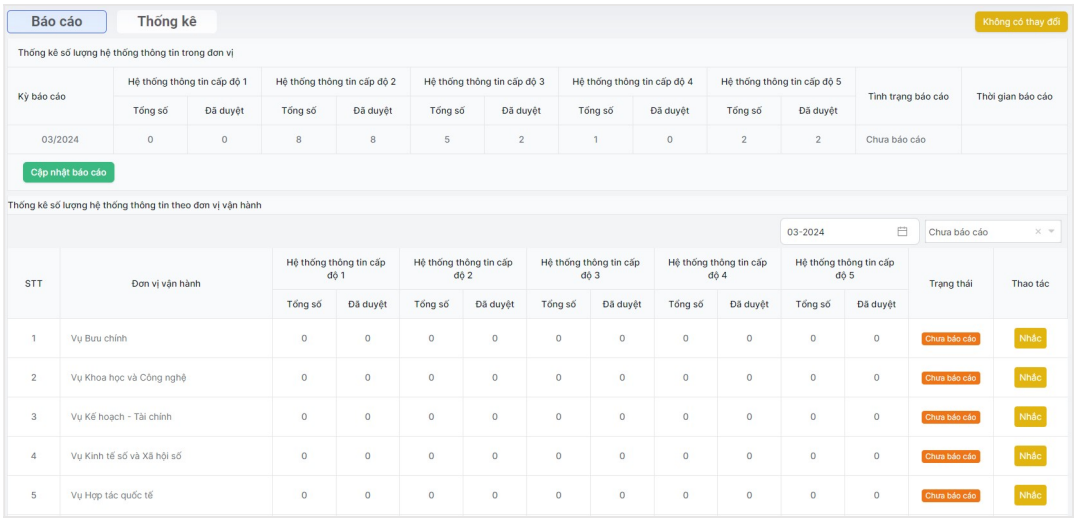
Báo cáo số liệu

Mục đích: Hiển thị thống kê số lượng HTTT trong đơn vị, tình trạng báo cáo theo các kỳ của đơn vị. Người dùng các đơn vị có thể gửi báo cáo số liệu HTTT lên cục ATTT phụ trách

Thao tác:

Bước 1: Từ menu trái chọn Báo cáo để chuyển đến màn "Báo cáo số liệu hệ thống thông tin"

Bước 2: Màn "**Báo cáo số liệu hệ thống thông tin**" hiển thị thống kê số liệu HTTT trong đơn vị danh sách HTTT trong đơn vị.

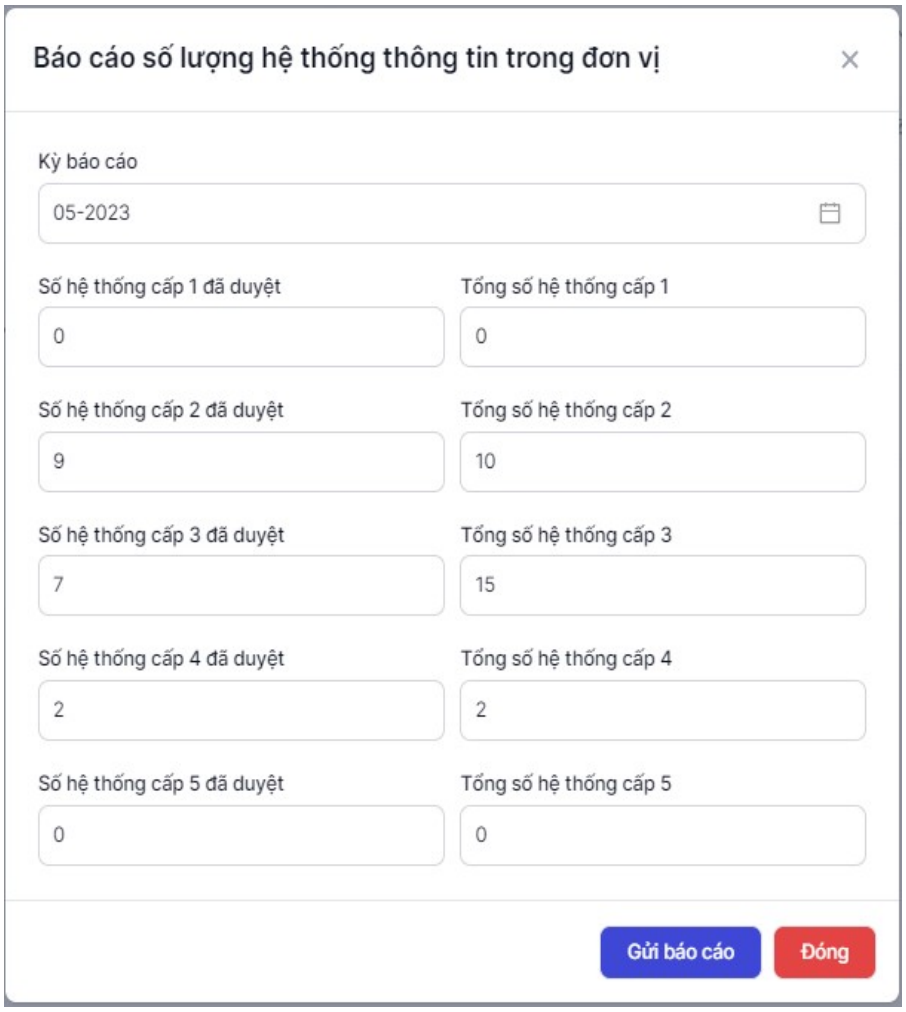


Hình 10: Màn thống kê số liệu HTTT và danh sách HTTT trong đơn vị

Bước 3: Chọn Cập nhật báo cáo để gửi số liệu báo cáo lên đơn vị phụ trách (Cục ATTT)

Bước 4: Nếu kỳ báo cáo không có thay đổi so với kỳ trước, chọn Không có thay đổi để gửi báo

cáo. Số liệu được tính tự động theo danh sách HTTT của đơn vị. Chọn Gửi báo cáo để gửi số liệu báo cáo lên đơn vị phụ trách(Cục ATTT)



Hình 11: Màn minh họa báo cáo không có thay đổi

Thống kê đơn vị

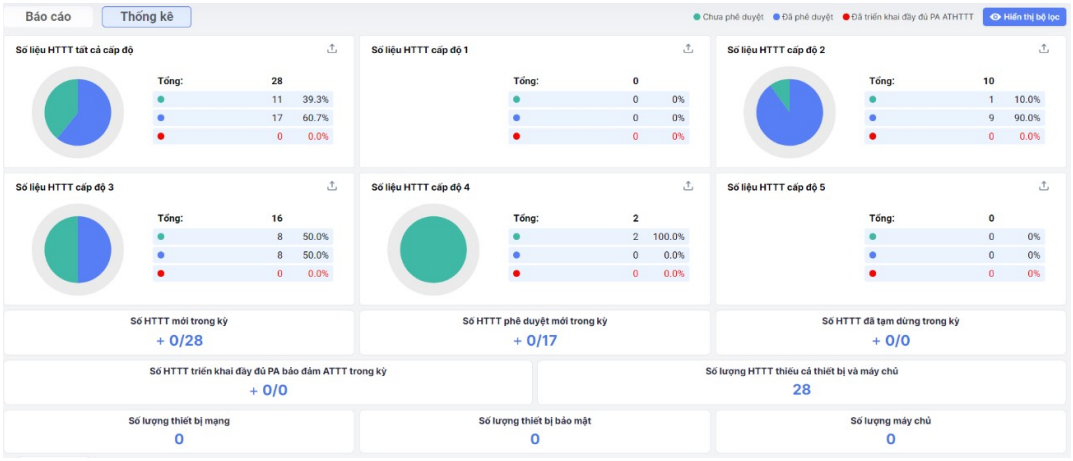
Mục đích: Cung cấp thông tin thống kê số lượng, thiết bị, máy chủ, phê duyệt mới, triển khai HTTT trong đơn vị

Thao tác:

Bước 1: Từ menu trái chọn 

để chuyển đến màn "**Thống kê hệ thống thông tin**"

Bước 2: Màn "**Thống kê hệ thống thông tin**" hiển thị thống kê , số liệu HTTT trong đơn vị.



Hình 12: Màn thống kê HTTT .

c) Quản lý hệ thống thông tin

Danh sách hệ thống thông tin

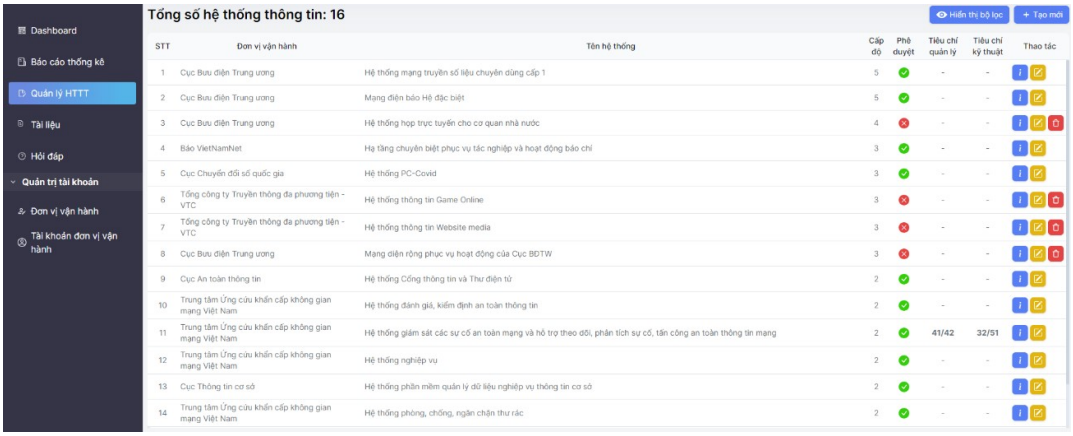
Mục đích: Chức năng này giúp người dùng xem tổng thể danh sách HTTT trong đơn vị, tìm kiếm HTTT theo tên hoặc theo cấp độ HTTT

Thao tác:

Bước 1: Từ màn hình "**Quản lý người dùng**" chọn nút 

để chuyển đến màn danh sách HTTT

Bước 2: Tại màn hình "**Danh sách hệ thống thông tin**" hiển thị tổng thể danh sách HTTT trong đơn vị.



Hình 13: Màn danh sách hệ thống thông tin

- Người dùng có thể lọc danh sách HTTT theo các cấp độ hệ thống, đơn vị vận hành, trạng thái phê duyệt, thông tin hiện trạng, tình trạng triển khai đầy đủ phương án ATTT, hoặc tra cứu theo tên HTTT

Hình 14: Mục tra cứu danh sách hệ thống thông tin

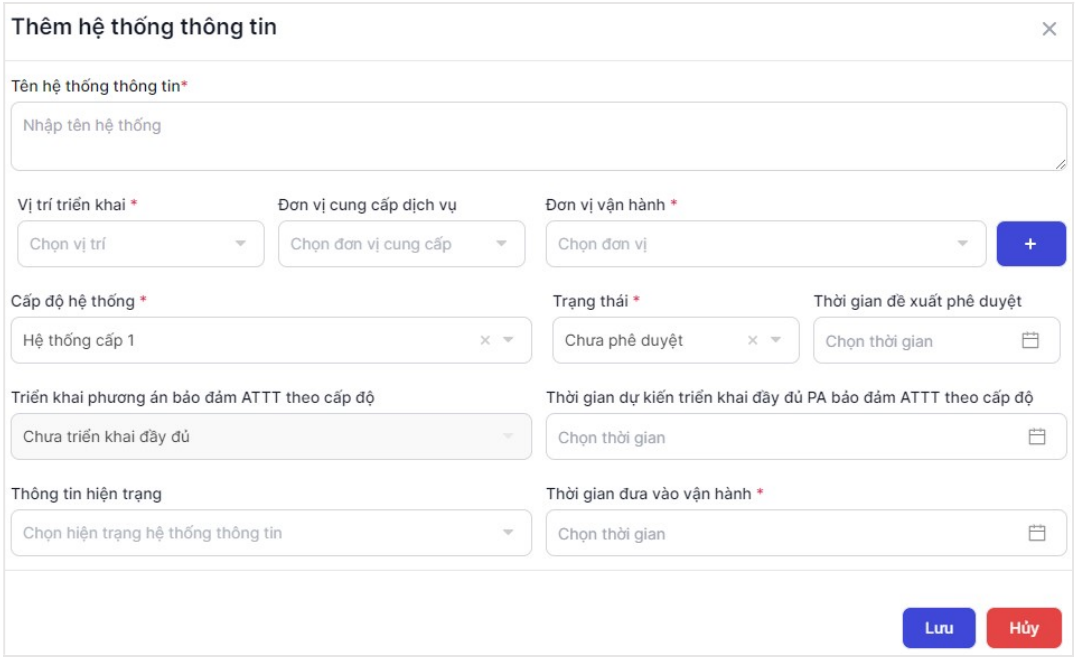
- Người dùng cũng có thể xem thông tin chi tiết HTTT, chọn để cập nhật thông tin HTTT hoặc chọn để chuyển HTTT sang danh sách dừng vận hành, hoặc để vận hành lại HTTT

Thêm mới hệ thống thông tin

Mục đích: Chức năng này giúp người dùng thêm mới HTTT

Thao tác:

Bước 1: Từ menu bên trái chọn Danh mục Hệ thống, người dùng di chuyển sang tay phải màn hình chọn + Tạo mới để người dùng nhập các thông tin về HTTT cần tạo



Hình 15: Màn thêm mới hệ thống thông tin

- **"Tên hệ thống thông tin"**: Nhập tên của HTTT
- **"Vị trí triển khai":** Nhập vị trí triển khai hệ thống(Tại cơ sở hoặc thuê dịch vụ)
- **"Đơn vị cung cấp dịch vụ":** chọn đơn vị cung cấp nếu hệ thống triển khai tại doanh nghiệp
- **"Đơn vị vận hành":** Nhập tên đơn vị vận hành hệ thống
- **"Cấp độ hệ thống":** Chọn cấp độ của hệ thống
- **"Trạng thái":** Nhập trạng thái phê duyệt hệ thống

- **"Thời gian đề xuất":** Nhập thời gian đề xuất nếu hệ thống chưa phê duyệt
- **"Thời gian dự kiến triển khai đầy đủ PA ATTT":** Nhập thời gian dự kiến
- **"Thông tin hiện trạng ":** Chọn hiện trạng hệ thống thông tin
- **"Thời gian đưa vào vận hành":** Người dùng chọn thời gian bắt đầu sử dụng hệ thống

Bước 3: Chọn 

để lưu thông tin HTTT vừa nhập

Cập nhật hệ thống thông tin

Mục đích: Chức năng này giúp người dùng cập nhật thông tin hồ sơ đề xuất cấp độ của HTTT

Thao tác:

Bước 1: Từ danh sách HTTT di chuột sang tay phải màn hình chọn  để cập nhật thông tin về HTTT, hệ thống sẽ điều hướng sang màn hình xây dựng hồ sơ đề xuất cấp độ để người dùng tiến hành cập nhật

Hình 16: Màn hình cập nhật hệ thống thông tin

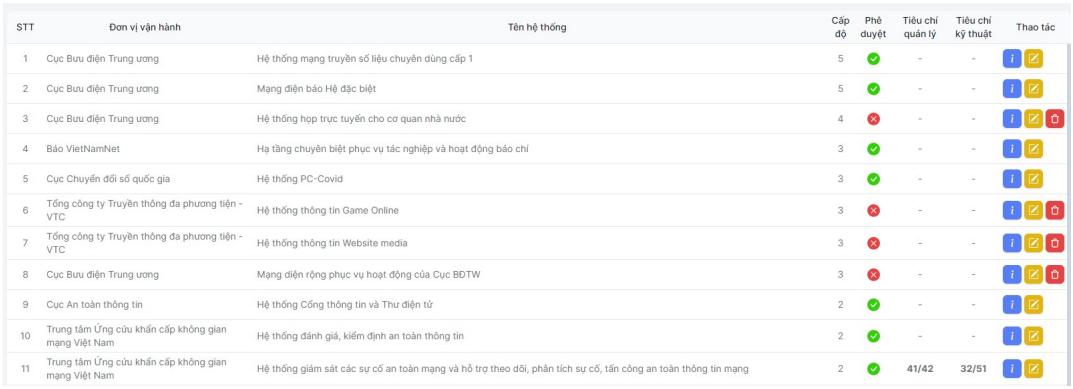
Bước 2: Chọn tạo mới hoặc sử dụng hồ sơ mẫu đã có để bắt đầu xây dựng hồ sơ đề xuất cấp độ

Chi tiết hệ thống thông tin

Mục đích: Chức năng này giúp người dùng xem danh sách HTTT đã duyệt trong đơn vị, tìm kiếm HTTT theo tên hoặc theo cấp độ HTTT

Thao tác:

Bước 1: Từ danh sách HTTT, click chọn vào nút  của dòng HTTT để xem chi tiết thông tin về HTTT



STT	Đơn vị vận hành	Tên hệ thống	Cấp độ	Phê duyệt	Tiêu chí quản lý	Tiêu chí kỹ thuật	Thao tác
1	Cục Bưu điện Trung ương	Hệ thống mạng truyền số liệu chuyên dùng cấp 1	5	✓	-	-	
2	Cục Bưu điện Trung ương	Mạng điện báo Hệ đặc biệt	5	✓	-	-	
3	Cục Bưu điện Trung ương	Hệ thống họp trực tuyến cho cơ quan nhà nước	4	✗	-	-	
4	Báo VietNamNet	Hạ tầng chuyên biệt phục vụ tác nghiệp và hoạt động báo chí	3	✓	-	-	
5	Cục Chuyển đổi số quốc gia	Hệ thống PC-Covid	3	✓	-	-	
6	Tổng công ty Truyền thông đa phương tiện - VTC	Hệ thống thông tin Game Online	3	✗	-	-	
7	Tổng công ty Truyền thông đa phương tiện - VTC	Hệ thống thông tin Website media	3	✗	-	-	
8	Cục Bưu điện Trung ương	Mạng diện rộng phục vụ hoạt động của Cục BĐTW	3	✗	-	-	
9	Cục An toàn thông tin	Hệ thống Cổng thông tin và Thư điện tử	2	✓	-	-	
10	Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam	Hệ thống đánh giá, kiểm định an toàn thông tin	2	✓	-	-	
11	Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam	Hệ thống giám sát các sự cố an toàn mạng và hỗ trợ theo dõi, phân tích sự cố, tấn công an toàn thông tin mạng	2	✓	41/42	32/51	

Hình 17: Màn danh sách hệ thống thông tin

Bước 2: Màn thông tin chi tiết HTTT, người dùng có thể xem thông tin và cập nhật các tài liệu liên quan của HTTT

Hình 18: Màn chi tiết hệ thống thông tin

d) Hồ sơ đề xuất cấp độ

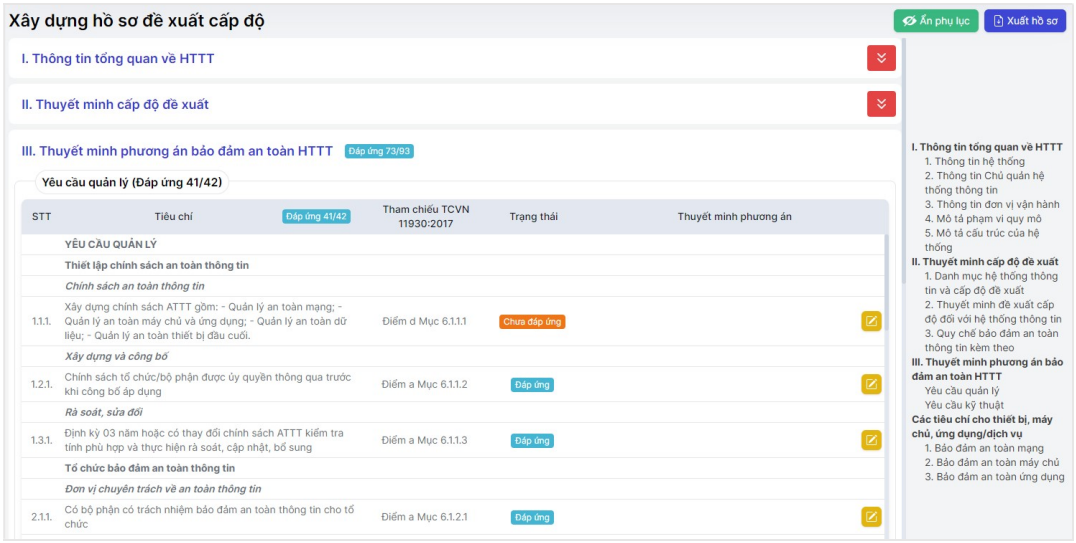
Xây dựng HSĐXCĐ cho HTTT

Mục đích: Chức năng này giúp người dùng xây dựng hồ sơ đề xuất các cấp độ trong HTTT

Thao tác:

Bước 1: Từ màn danh sách HTTT chọn  để chuyển đến màn "Xây dựng hồ sơ đề xuất cấp độ"

Bước 2 : Màn "Xây dựng sơ đề xuất cấp độ" hiển thị



Hình 19: Màn xây dựng dự thảo hồ sơ đề xuất cấp độ

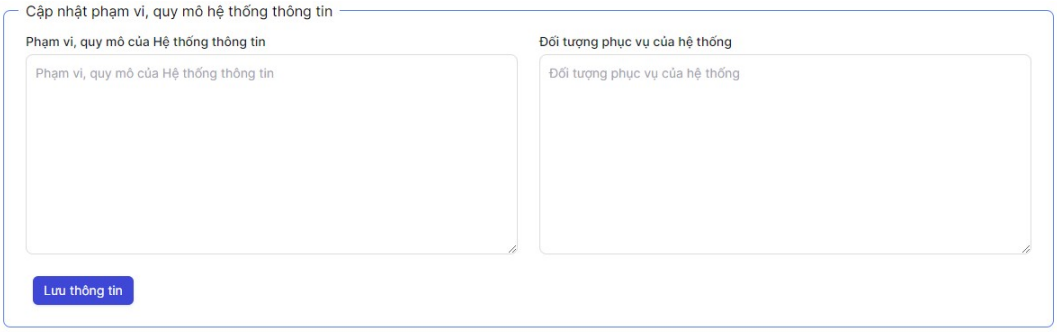
Người dùng thao tác nhấn nút » hoặc click các mục trên phụ lục để cập nhật thông tin của HTTT

Mô tả phạm vi quy mô

Mục đích: Cập nhật phạm vi, quy mô của HTTT

Thao tác:

Bước 1: Từ màn hình HSĐXCĐ, tại mục 4. Mô tả phạm vi quy mô chọn Cập nhật thông tin



Hình 20: Màn phạm vi, quy mô HTTT hồ sơ đề xuất cấp độ

Bước 2: Nhập thông tin và chọn Lưu thông tin

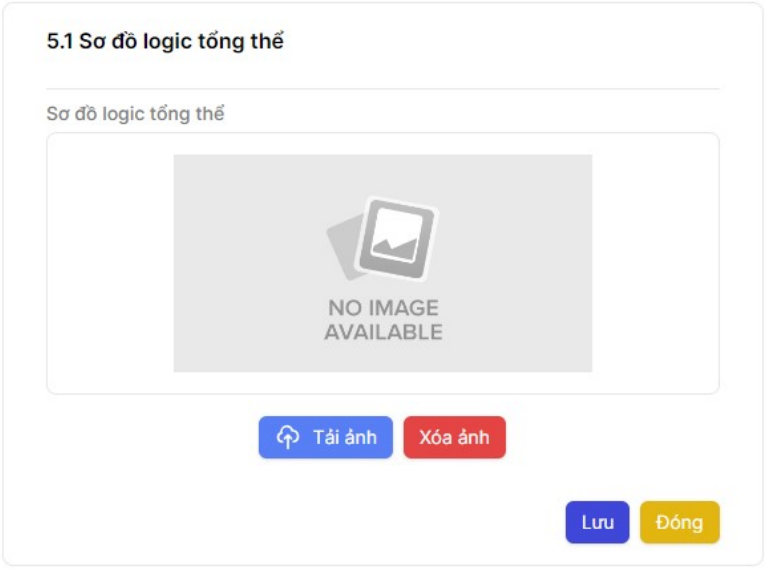
Mô tả cấu trúc của hệ thống

Mục đích: Chức năng này giúp người dùng cập nhật các sơ đồ logic và sơ đồ kết nối vật lý của HTTT

Thao tác:

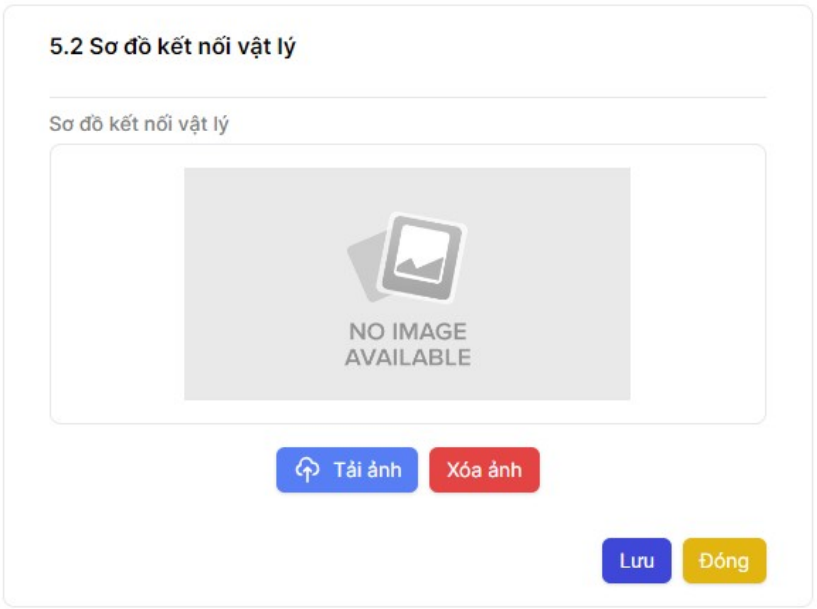
Bước 1: Từ màn hình HSĐXCĐ, tại mục 4. Mô tả phạm vi quy mô chọn Cập nhật từng sơ đồ của hệ thống

Bước 2: Tải ảnh sơ đồ logic tổng thể của hệ thống và nhấn lưu



Hình 21: Màn hình sơ đồ logic tổng thể

Bước 3: Tải ảnh sơ đồ kết nối vật lý của hệ thống và nhấn lưu



Hình 22: Màn hình sơ đồ kết nối vật lý

Thiết kế các vùng mạng

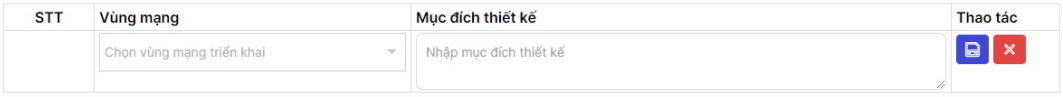
Mục đích: Chức năng này giúp người dùng cập nhật danh sách các vùng mạng trong HTTT

Thao tác:

Bước 1: Từ màn hình HSĐXCĐ, tại mục 5.3 Thiết kế các vùng mạng, chọn Thêm vùng mạng

Hình 23: Màn danh sách vùng mạng trong HTTT

Bước 2: Chọn vùng mạng sử dụng và nhập mục đích sử dụng



Hình 24: Màn thêm vùng mạng trong HTTT

- **"Vùng mạng"**: Chọn vùng mạng mới
- **"Mục đích thiết kế":** Nhập thông tin mục đích

Bước 3: Chọn  để lưu thông tin thiết bị vừa nhập

Bước 4: Người dùng cũng có thể chọn  để sửa thông tin thiết bị, hoặc chọn  để xóa thiết bị khỏi danh sách

Danh mục thiết bị mạng/bảo mật sử dụng trong hệ thống

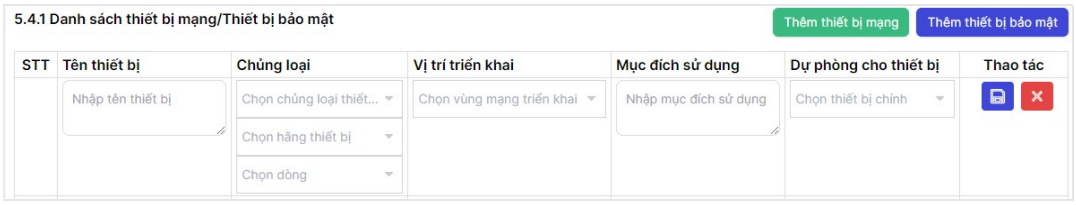
<u>Mục đích:</u> Chức năng này giúp người dùng cập nhật danh sách các thiết bị trong HTTT

<u>Thao tác:</u>

Bước 1: Từ màn hình HSĐXCĐ, tại mục 5.4.1 Danh mục thiết bị mạng/bảo mật sử dụng trong hệ thống hiển thị danh sách thiết bị mạng, thiết bị bảo mật được sử dụng trong HTTT

Hình 25: Màn danh sách thiết bị mạng, bảo mật trong HTTT

Bước 2: Người dùng có thể chọn thêm mới hoặc cập nhật các thiết bị trong HTTT



Hình 26: Màn thêm mới thiết bị trong HTTT

- **"Tên thiết bị"**: Nhập tên của thiết bị
- **"Chủng loại"**: Chọn chủng loại thiết bị
- **"Hãng thiết bị"**: Chọn hãng thiết bị
- **"Model"**: Chọn dòng thiết bị theo hãng
- **"Vị trí triển khai"**: Nhập vị trí đặt thiết bị
- **"Mục đích sử dụng"**: Mục đích sử dụng của thiết bị
- **"Dự phòng cho thiết bị"**: Chọn thiết bị chính cần dự phòng(Nếu đang nhập thiết bị dự phòng)

Bước 3: Chọn để lưu thông tin thiết bị vừa nhập

Bước 4: Người dùng cũng có thể chọn để sửa thông tin thiết bị, hoặc chọn để xóa thiết bị khỏi danh sách

Danh mục thiết bị máy chủ trong hệ thống

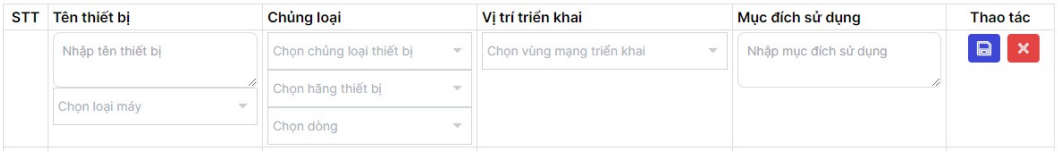
Mục đích: Chức năng này giúp người dùng cập nhật danh sách các thiết bị máy chủ trong HTTT

Thao tác:

Bước 1: Từ màn hình HSĐXCĐ, tại mục 5.4.2 Danh mục thiết bị máy chủ sử dụng trong hệ thống hiển thị danh sách thiết máy chủ được sử dụng trong HTTT

Hình 27: Màn danh sách thiết bị máy chủ trong HTTT

Bước 2: Người dùng có thể chọn thêm mới hoặc cập nhật các thiết bị trong HTTT



Hình 28: Màn thêm mới thiết bị máy chủ trong HTTT

- **"Tên thiết bị"**: Nhập tên của thiết bị
- **"Loại máy"**: Chọn loại máy vật lý hoặc máy chủ ảo hóa
- **"Chủng loại"**: Chọn chủng loại thiết bị
- **"Hãng thiết bị"**: Chọn hãng thiết bị
- **"Model"**: Chọn dòng thiết bị theo hãng
- **"Vị trí triển khai"**: Nhập vị trí đặt thiết bị
- **"Mục đích sử dụng"**: Mục đích sử dụng của thiết bị

Bước 3: Chọn để lưu thông tin thiết bị vừa nhập

Bước 4: Người dùng cũng có thể chọn để sửa thông tin thiết bị, hoặc chọn để xóa thiết bị khỏi danh sách

Danh sách dịch vụ

Mục đích: Chức năng này giúp người dùng cập nhật danh sách các dịch vụ trong HTTT

Thao tác:

Bước 1: Từ màn hình HSĐXCĐ, tại mục 5.5 Danh mục các ứng dụng/dịch vụ cung cấp bởi hệ thống hiển thị danh sách ứng dụng cài đặt trên máy chủ trong HTTT

Bước 2: Danh sách dịch vụ hiển thị các dịch vụ, ứng dụng được sử dụng trong HTTT

Hình 29: Màn danh sách dịch vụ thuộc HTTT

Bước 3: Người dùng có thể thêm mới các dịch vụ vào HTTT

Hình 30: Màn thêm mới dịch vụ thuộc HTTT

- **"Tên dịch vụ"**: Nhập tên dịch vụ
- **"Máy chủ"**: Chọn loại máy chủ

- **"Ứng dụng cài đặt"**: Nhập tên ứng dụng cài đặt
- **"Vùng mạng"**: Chọn vùng mạng
- **"Hệ điều hành"**: Nhập tên hệ diều hành
- **"Mục đích sử dụng"**: Nhập mục đích sử dụng

Bước 4 : Chọn để lưu thông tin thiết bị vừa nhập

Bước 5: Người dùng cũng có thể chọn để sửa thông tin thiết bị, hoặc chọn để xóa dịch vụ khỏi danh sách

Danh sách IP vùng mạng

Mục đích: Chức năng này giúp người dùng xem danh sách IP vùng mạng, tìm kiếm HTTT theo tên hoặc theo cấp độ HTTT

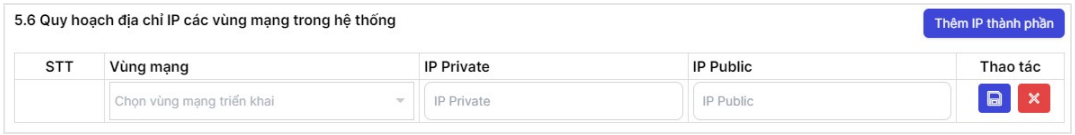
Thao tác:

Bước 1: Từ màn hình HSĐXCĐ, tại mục 5.6 Quy hoạch địa chỉ IP các vùng mạng trong hệ thống

Bước 2: Danh sách IP vùng mạng hiển thị các IP được sử dụng trong HTTT

Hình 31: Màn danh sách IP thuộc HTTT

Bước 3: Người dùng có thể chọn Thêm IP thành phần để mới IP của HTTT



Hình 32: Màn thêm mới địa chỉ IP

- **"Vị trí triển khai"**: Nhập vị trí đặt thiết bị
- **"IP Public"**: IP công khai
- **"IP Private"**: IP bảo mật

Bước 4: Chọn nút Lưu lại để lưu lại danh sách thông tin IP đã cập nhật

Danh mục máy trạm trong HTTT

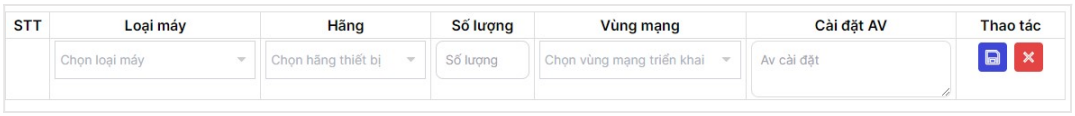
Mục đích: Chức năng này giúp người dùng cập nhật danh sách các thiết bị máy trạm trong HTTT

Thao tác:

Bước 1: Từ màn hình HSĐXCĐ, tại mục 5.4.2 Danh mục thiết bị máy chủ sử dụng trong hệ thống hiển thị danh sách thiết máy chủ được sử dụng trong HTTT

Hình 33: Màn danh sách thiết bị máy trạm trong HTTT

Bước 2: Người dùng có thể chọn thêm mới hoặc cập nhật các thiết bị trong HTTT



Hình 34: Màn thêm mới thiết bị trong HTTT

- **"Loại máy"**: Chọn loại máy PC hoặc máy laptop
- **"Hãng thiết bị"**: Chọn hãng thiết bị
- **"Số lượng"**: Chọn số lượng thiết bị theo hãng
- **"Vùng mạng"**: Nhập vùng mạng sử dụng
- **"Cài đặt AV"**: Thông tin phần mềm AV cài đặt trên máy

Bước 3: Chọn để lưu thông tin thiết bị vừa nhập

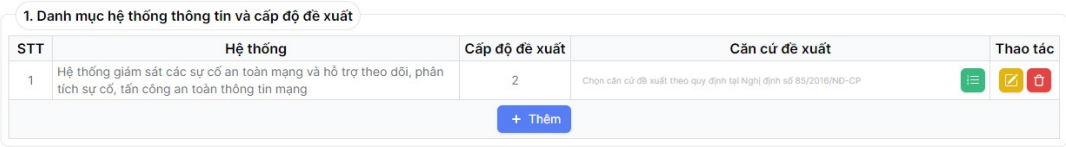
Bước 4: Người dùng cũng có thể chọn để sửa thông tin thiết bị, hoặc chọn để xóa thiết bị khỏi danh sách

Danh mục hệ thống thông tin và cấp độ đề xuất

Mục đích: Chức năng này giúp người dùng cập nhật danh sách các hệ thống thành phần trong HTTT

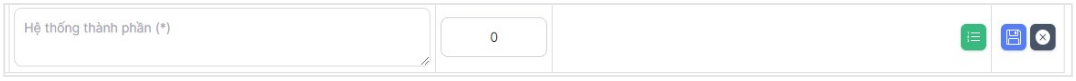
Thao tác:

Bước 1: Từ màn hình HSĐXCĐ, tại phần II mục 1 Danh mục hệ thống thông tin và cấp độ đề xuất hiển thị danh sách hệ thống thành phần trong HTTT

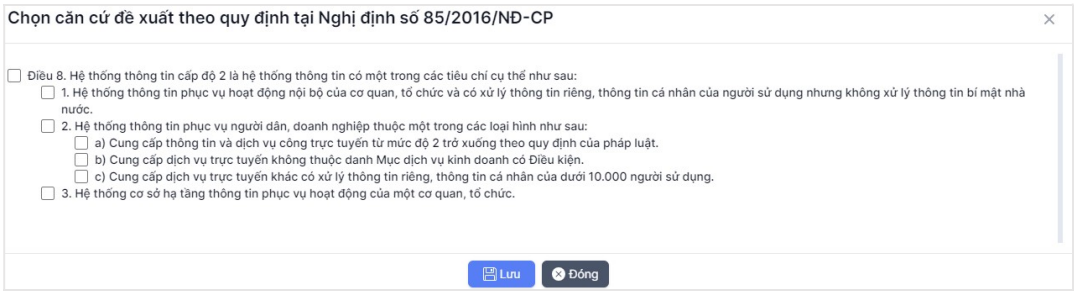


Hình 35: Màn danh sách hệ thống thành phần trong HTTT

Bước 2: Người dùng có thể chọn thêm mới hoặc cập nhật các hệ thống thành phần trong HTTT



Hình 36: Màn thêm mới hệ thống thành phần trong HTTT



Hình 37: Màn chọn căn cứ đề xuất theo cấp độ của HTTT

- **"Hệ thống thành phần"**: Nhập tên hệ thống thành phần
- **"Cấp độ đề xuất"**: Chọn cấp độ của hệ thống thành phần
- **"Căn cứ đề xuất"**: Chọn các căn cứ đề xuất

Bước 3: Chọn  để lưu thông tin thiết bị vừa nhập

Bước 4: Người dùng cũng có thể chọn  để sửa thông tin thiết bị, hoặc chọn  để xóa thiết bị khỏi danh sách

Thuyết minh đề xuất cấp độ đối với hệ thống thông tin

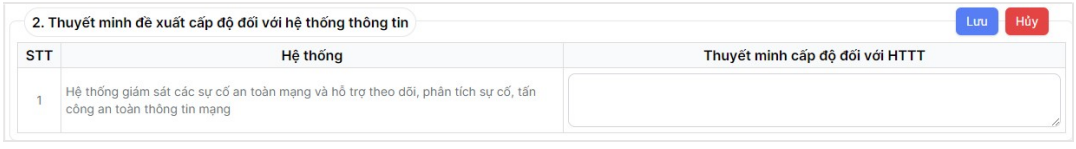
<u>Mục đích:</u> Chức năng này giúp người dùng cập nhật danh sách các thuyết minh đề xuất cấp độ các hệ thống trong HTTT

<u>Thao tác:</u>

Bước 1: Từ màn hình HSĐXCĐ, tại phần II mục 2 Thuyết minh đề xuất cấp độ đối với HTTT hiển thị danh sách thuyết minh hệ thống thành phần trong HTTT

Hình 38: Màn danh sách thuyết minh hệ thống thành phần trong HTTT

Bước 2: Người dùng có thể cập nhật các thuyết minh hệ thống thành phần trong HTTT



Hình 39: Màn cập nhật thuyết minh hệ thống thành phần trong HTTT

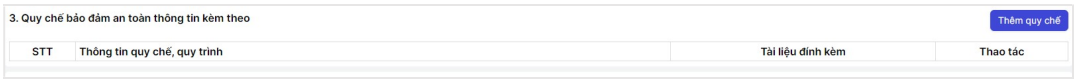
Bước 3: Chọn Lưu để lưu thông tin thiết bị vừa nhập

Quy chế bảo đảm an toàn thông tin kèm theo

Mục đích: Chức năng này giúp người dùng cập nhật danh sách các quy chế trong HTTT

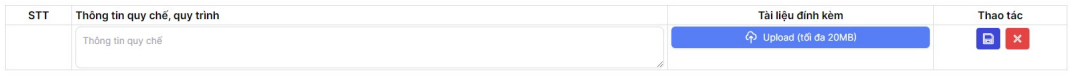
Thao tác:

Bước 1: Từ màn hình HSĐXCĐ, tại phần II mục 3 Danh mục quy chế đảm bảo ATTT trong HTTT



Hình 40: Màn danh sách quy chế trong HTTT

Bước 2: Người dùng có thể chọn thêm mới hoặc cập nhật các quy chế trong HTTT



Hình 41: Màn thêm mới quy chế trong HTTT

- **"Thông tin quy chế"**: Nhập tên thông tin quy chế hệ thống thông tin
- **"Tài liệu đính kèm"**: upload tài liệu liên quan

Bước 3: Chọn để lưu thông tin vừa nhập

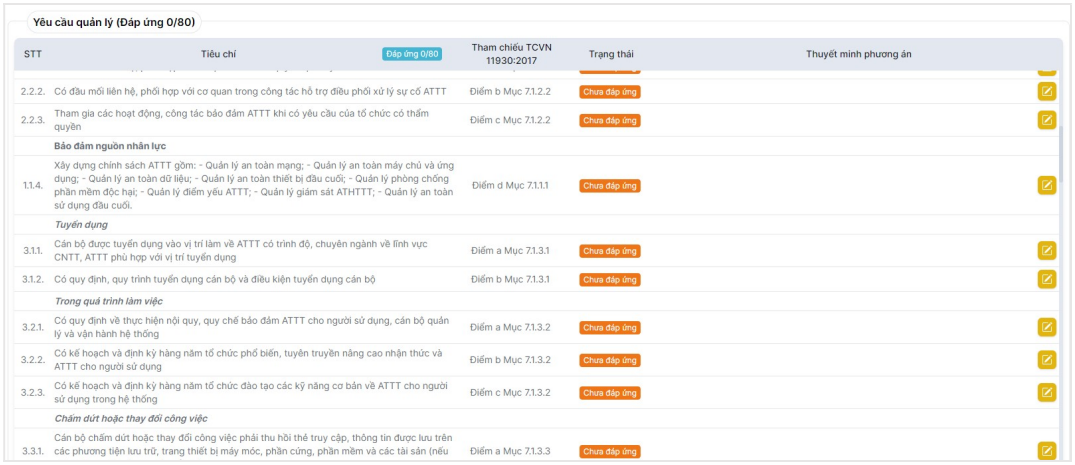
Bước 4: Người dùng cũng có thể chọn để sửa thông tin, hoặc chọn để xóa tài liệu khỏi danh sách

Phương án bảo đảm an toàn HTTT - Yêu cầu quản lý

Mục đích: Người dùng cập nhật lại thông tin thuyết minh các phương án đảm bảo ATHTTT

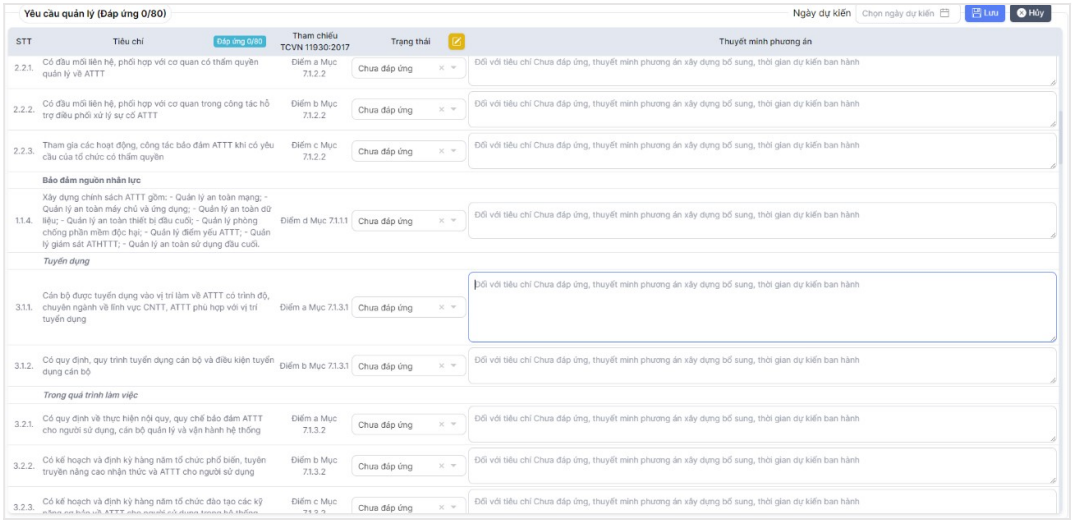
Thao tác:

Bước 1: Từ màn hình HSĐXCĐ, tại phần III. Thuyết minh phương án bảo đảm an toàn HTTT, hiển thị mục Yêu cầu quản lý



Hình 42: Màn danh sách Yêu cầu quản lý Phương án đảm bảo an toàn HTTT

Bước 2: Người dùng có thể cập nhật từng tiêu chí đáp ứng của HTTT



Hình 43: Màn cập nhật Phương án triển khai

- **"Trạng thái "**: Chọn trạng thái đáp ứng tiêu chí
- **"Ngày dự kiến"**: Nếu chưa đáp ứng, chọn thời gian dự kiến
- **"Phương án"**: Ghi chú về thông tin phương án

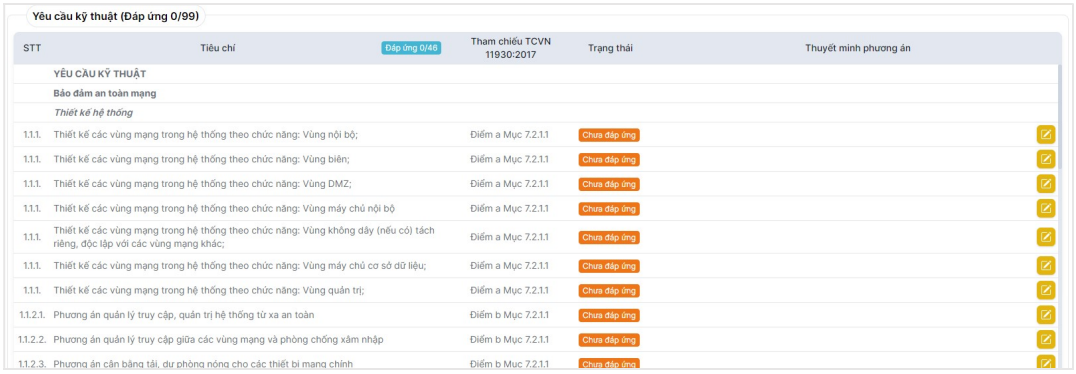
Bước 3: Chọn nút Lưu để lưu lại danh sách thông tin tiêu chí đã cập nhật

Phương án bảo đảm an toàn HTTT - Yêu cầu quản lý

<u>Mục đích:</u> Người dùng cập nhật lại thông tin thuyết minh các phương án đảm bảo ATHTTT

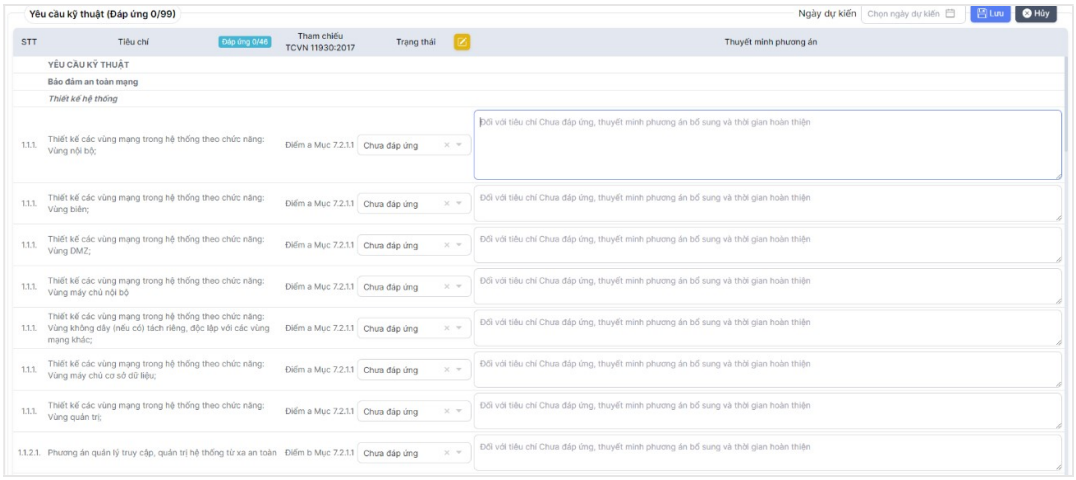
<u>Thao tác:</u>

Bước 1: Từ màn hình HSĐXCĐ, tại phần III. Thuyết minh phương án bảo đảm an toàn HTTT, hiển thị mục Yêu cầu kỹ thuật



Hình 44: Màn danh sách Yêu cầu kỹ thuật Phương án đảm bảo an toàn HTTT

Bước 2: Người dùng có thể cập nhật từng tiêu chí đáp ứng của HTTT



Hình 45: Màn cập nhật Phương án triển khai

- **"Trạng thái "**: Chọn trạng thái đáp ứng tiêu chí
- **"Ngày dự kiến"**: Nếu chưa đáp ứng, chọn thời gian dự kiến
- **"Phương án"**: Ghi chú về thông tin phương án

Bước 3: Chọn nút 

để lưu lại danh sách thông tin tiêu chí đã cập nhật

g) Tài liệu - Hỏi đáp

Tài liệu

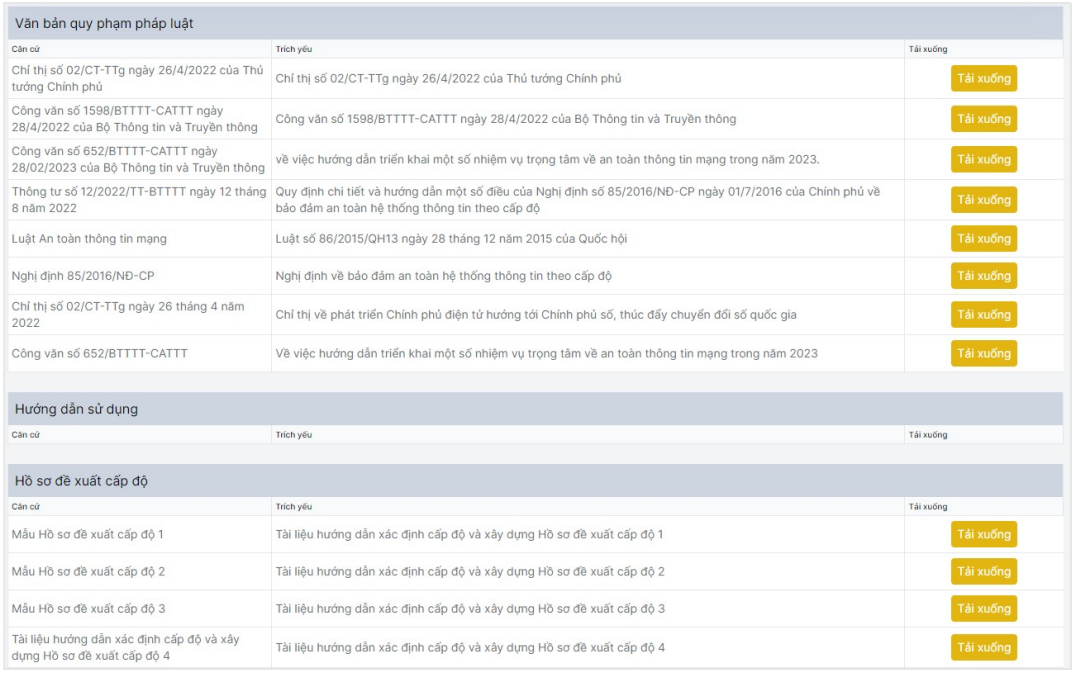
<u>Mục đích:</u> Hiển thị danh sách tài liệu quy phạm pháp luật, tài liệu hướng dẫn

<u>Thao tác</u>:

Bước 1: Từ menu trái chọn 

để chuyển đến màn "**Tài liệu**"

Bước 2: Màn "**Tài liệu**" hiển thị danh sách các tài liệu liên quan, được chia thành các nhóm: Văn bản quy phạm pháp luật, Hướng dẫn sử dụng, Hồ sơ đề xuất cấp độ, Biểu mẫu công văn



Văn bản quy phạm pháp luật

Căn cứ	Trích yếu	Tải xuống
Chỉ thị số 02/CT-TTg ngày 26/4/2022 của Thủ tướng Chính phủ	Chỉ thị số 02/CT-TTg ngày 26/4/2022 của Thủ tướng Chính phủ	Tải xuống
Công văn số 1598/BTTTT-CATTT ngày 28/4/2022 của Bộ Thông tin và Truyền thông	Công văn số 1598/BTTTT-CATTT ngày 28/4/2022 của Bộ Thông tin và Truyền thông	Tải xuống
Công văn số 652/BTTTT-CATTT ngày 28/02/2023 của Bộ Thông tin và Truyền thông	về việc hướng dẫn triển khai một số nhiệm vụ trọng tâm về an toàn thông tin mạng trong năm 2023.	Tải xuống
Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022	Quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ	Tải xuống
Luật An toàn thông tin mạng	Luật số 86/2015/QH13 ngày 28 tháng 12 năm 2015 của Quốc hội	Tải xuống
Nghị định 85/2016/NĐ-CP	Nghị định về bảo đảm an toàn hệ thống thông tin theo cấp độ	Tải xuống
Chỉ thị số 02/CT-TTg ngày 26 tháng 4 năm 2022	Chỉ thị về phát triển Chính phủ điện tử hướng tới Chính phủ số, thúc đẩy chuyển đổi số quốc gia	Tải xuống
Công văn số 652/BTTTT-CATTT	Về việc hướng dẫn triển khai một số nhiệm vụ trọng tâm về an toàn thông tin mạng trong năm 2023	Tải xuống

Hướng dẫn sử dụng

Căn cứ	Trích yếu	Tải xuống

Hồ sơ đề xuất cấp độ

Căn cứ	Trích yếu	Tải xuống
Mẫu Hồ sơ đề xuất cấp độ 1	Tài liệu hướng dẫn xác định cấp độ và xây dựng Hồ sơ đề xuất cấp độ 1	Tải xuống
Mẫu Hồ sơ đề xuất cấp độ 2	Tài liệu hướng dẫn xác định cấp độ và xây dựng Hồ sơ đề xuất cấp độ 2	Tải xuống
Mẫu Hồ sơ đề xuất cấp độ 3	Tài liệu hướng dẫn xác định cấp độ và xây dựng Hồ sơ đề xuất cấp độ 3	Tải xuống
Tài liệu hướng dẫn xác định cấp độ và xây dựng Hồ sơ đề xuất cấp độ 4	Tài liệu hướng dẫn xác định cấp độ và xây dựng Hồ sơ đề xuất cấp độ 4	Tải xuống

Hình 46: Màn danh sách tài liệu công văn

Bước 3: Người dùng đơn vị có thể tải các tài liệu để tham khảo

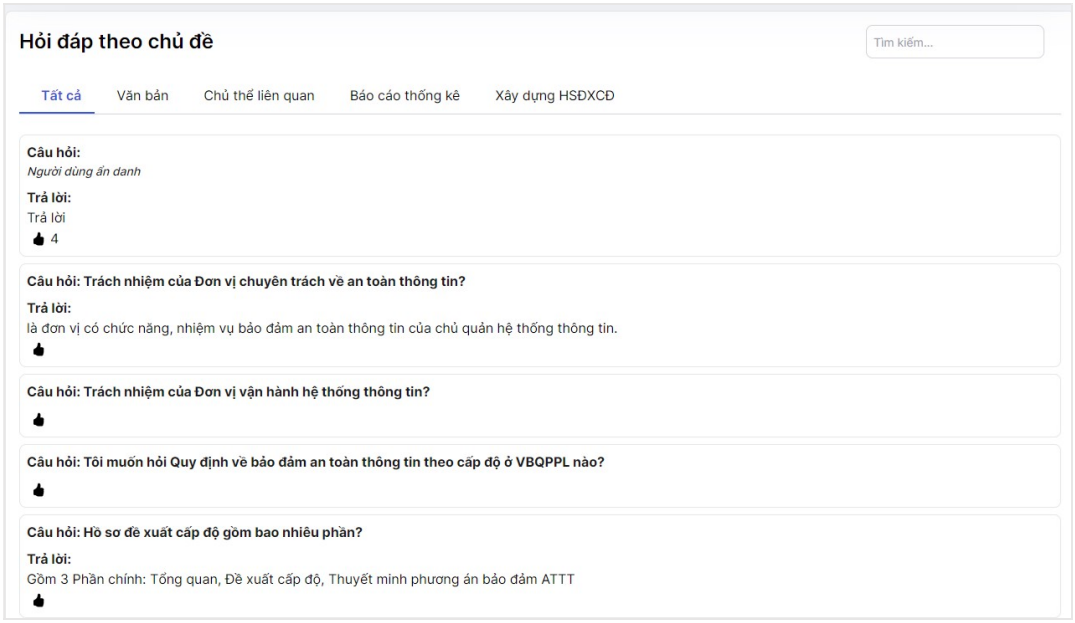
Hỏi đáp

Mục đích: Hiển thị danh sách các câu hỏi về các chủ đề liên quan trong hệ thống

Thao tác:

Bước 1: Từ menu trái chọn 

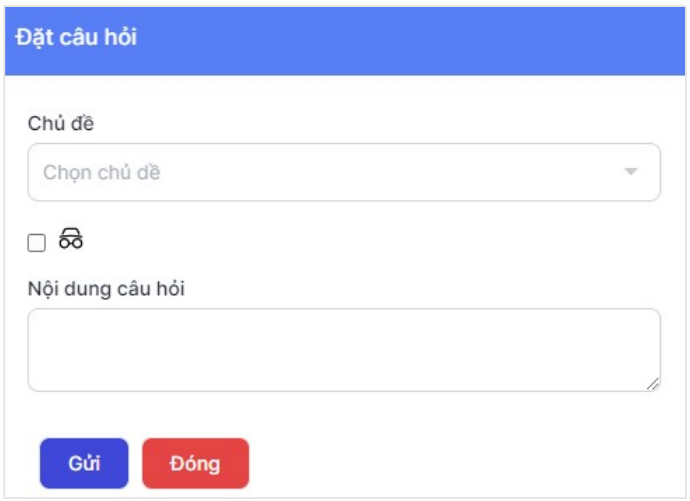
để chuyển đến màn "**Hỏi đáp theo chủ đề**"



Hình 47: Màn danh sách câu hỏi theo chủ đề

Bước 2: Người dùng đơn vị có thể lọc câu hỏi theo chủ đề hoặc tìm kiếm theo từ khóa

Bước 3: Để thêm mới "Tài khoản", người dùng chọn + Tạo mới ở phía bên phải.



Hình 48: Màn đăng ký câu hỏi

- **"Chủ đề"**: Chọn chủ đề cần hỏi
- **"Ẩn danh"**: Chọn nếu muốn hỏi ẩn danh
- **"Nội dung câu hỏi" :** Nhập vấn đề cần hỏi

Bước 4: Chọn Gửi để gửi thông tin câu hỏi lên hệ thống

Phụ lục 6
HƯỚNG DẪN SỬ DỤNG NỀN TẢNG ĐIỀU PHỐI XỬ LÝ SỰ CỐ AN TOÀN THÔNG TIN MẠNG QUỐC GIA

1. Hướng dẫn đăng ký, kết nối Nền tảng IRLab

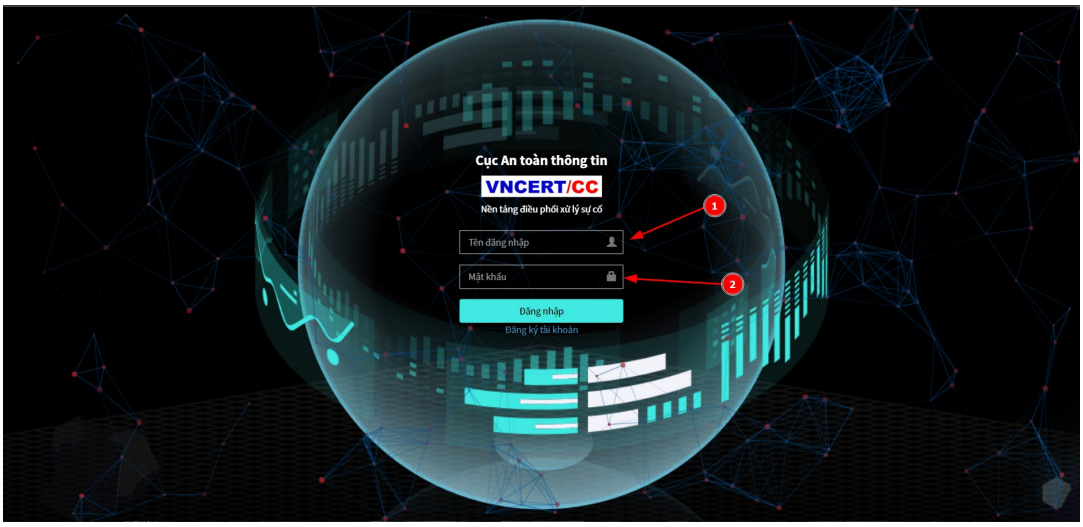
Bước 1: Các tổ chức, doanh nghiệp, cá nhân có nhu cầu sử dụng Nền tảng IRLab khai báo thông tin vào form đăng ký tại địa chỉ: https://irlab.vn/bot hoặc gửi văn bản đăng ký tài khoản IRLab tới Trung tâm VNCERT/CC.

Bước 2: Trung tâm VNCERT/CC sẽ xác nhận thông tin và gửi thông tin phản hồi cho đầu mối đăng ký của tổ chức từ địa chỉ irlab@vncert.vn.

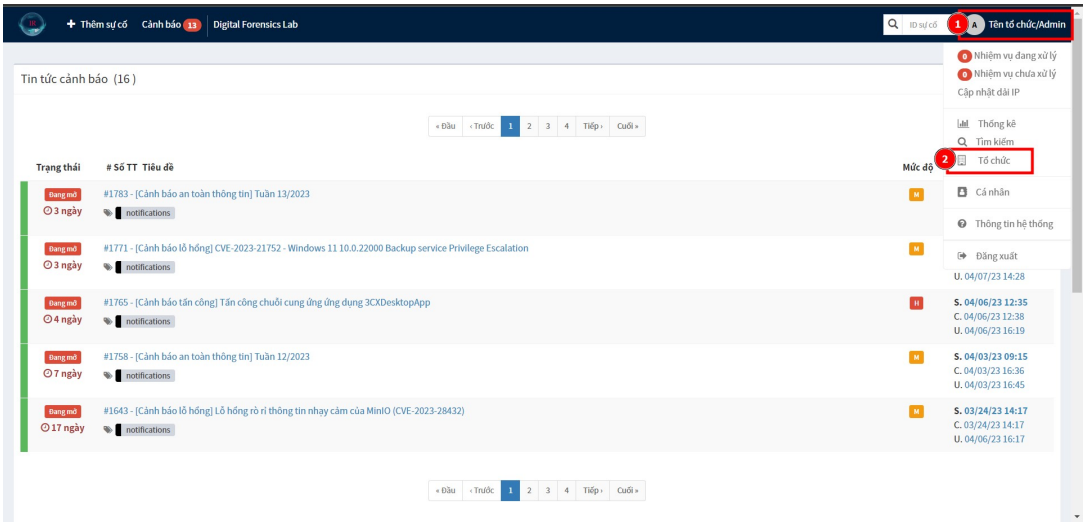
2. Hướng dẫn sử dụng Nền tảng IRLab

a) Lần đăng nhập đầu tiên

Khi đăng nhập lần đầu tiên, quản trị viên cần đăng nhập bằng thông tin đăng nhập đã được cung cấp:



Hình 1: Màn hình đăng nhập

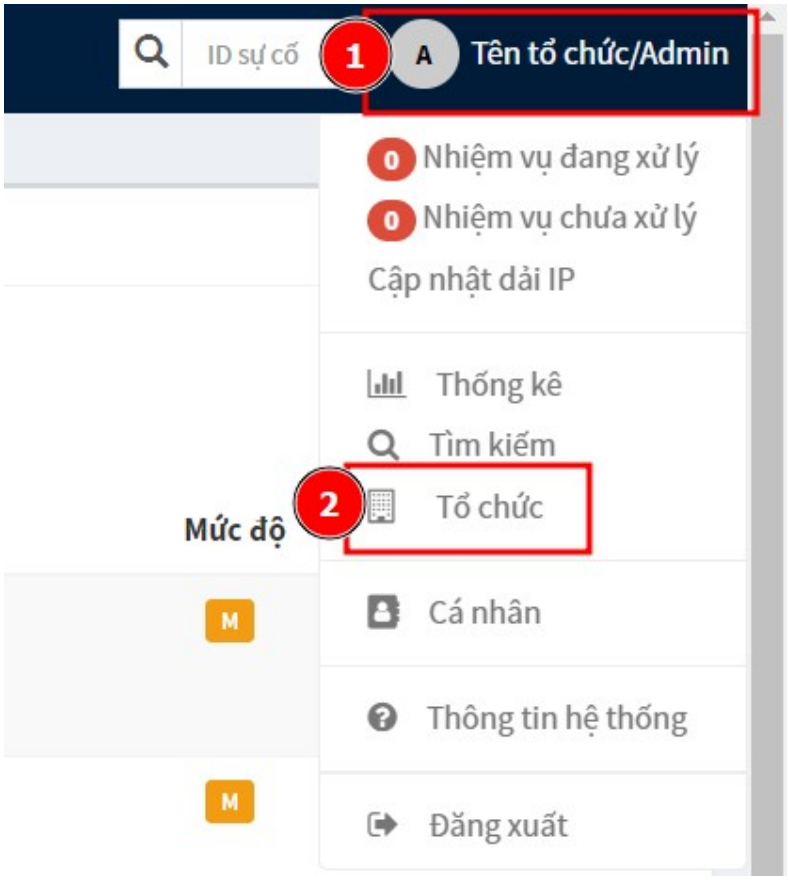


Hình 2: Màn hình danh sách các cảnh báo

b) Chức năng Tạo người dùng

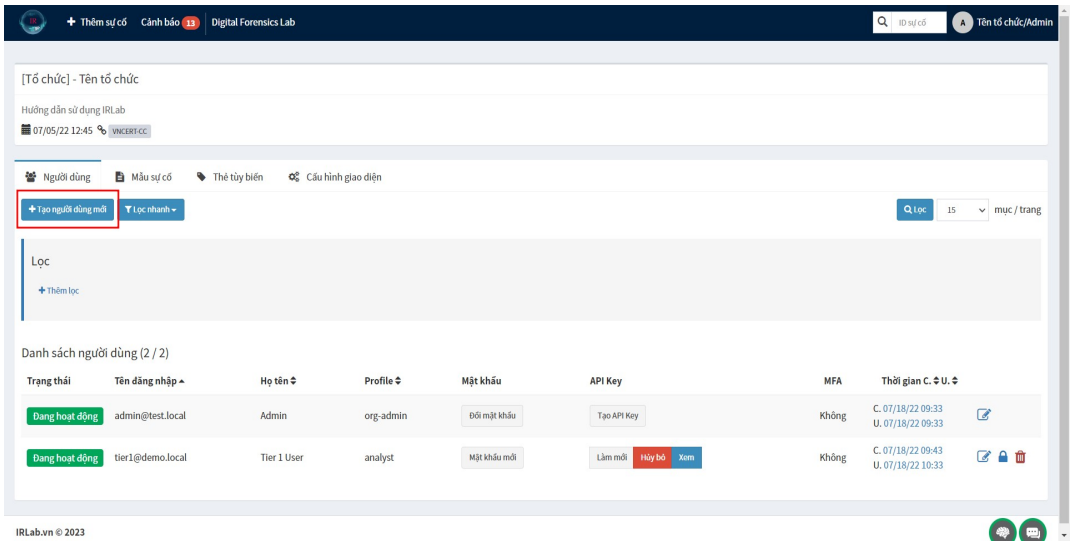
Người dùng có quyền quản trị sau khi click vào avatar sẽ thấy menu "Tổ chức" được dùng để quản lý:

- Người dùng
- Thẻ tuỳ biến
- Cài đặt giao diện

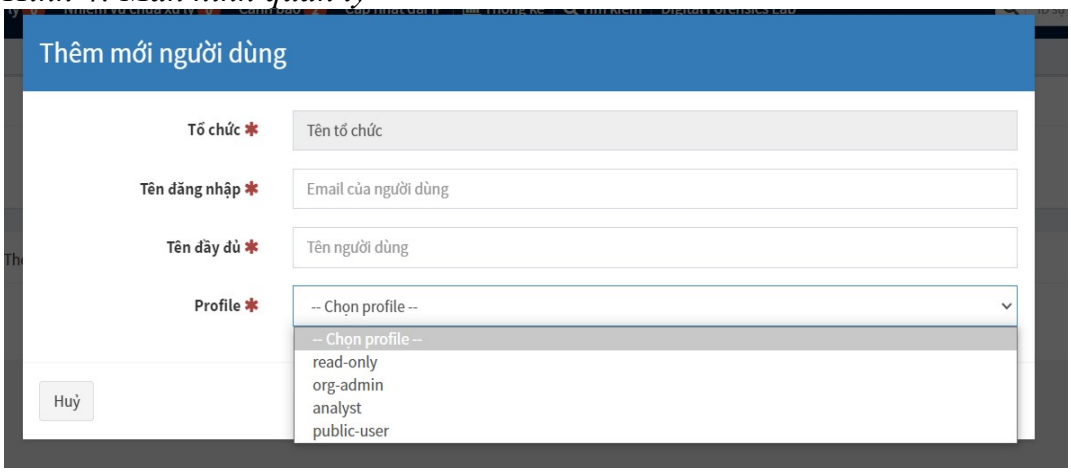


Hình 3: Màn hình quản lý

Để tạo một người dùng, cần nhấp vào nút "Tạo người dùng mới" để mở hộp thoại tạo người dùng.



Hình 4: Màn hình quản lý

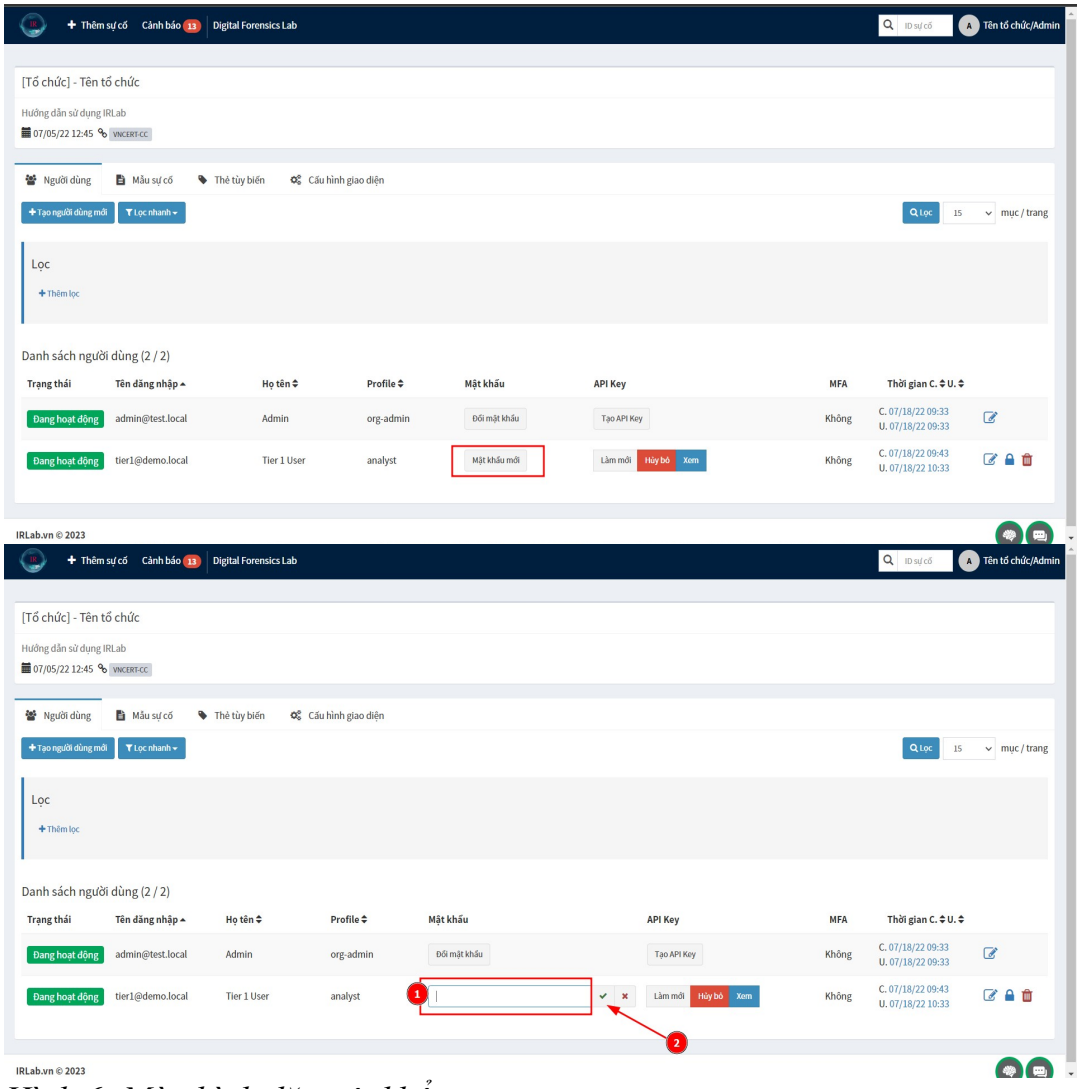


Hình 5: Màn hình thêm mới người dùng

Các loại tài khoản mà người quản trị của tổ chức có thể tạo:

- org-admin: Tất cả các quyền trong tổ chức (bao gồm các quyền của analyst và quyền quản lý người dùng, thẻ tuỳ chọn, …), có thể cập nhật địa chỉ Public IP của cơ quan để nhận báo cáo giám sát gián tiếp
- analyst: Có thể quản lý các sự cố và các đối tượng liên quan khác (đặc trưng, nhiệm vụ,…), có thể chia sẻ sự cố
- public-user: Chỉ được phép thêm sự cố và chia sẻ sự cố
- read-only: Không có quyền chỉnh sửa và tạo mới sự cố, chỉ có thể xem.

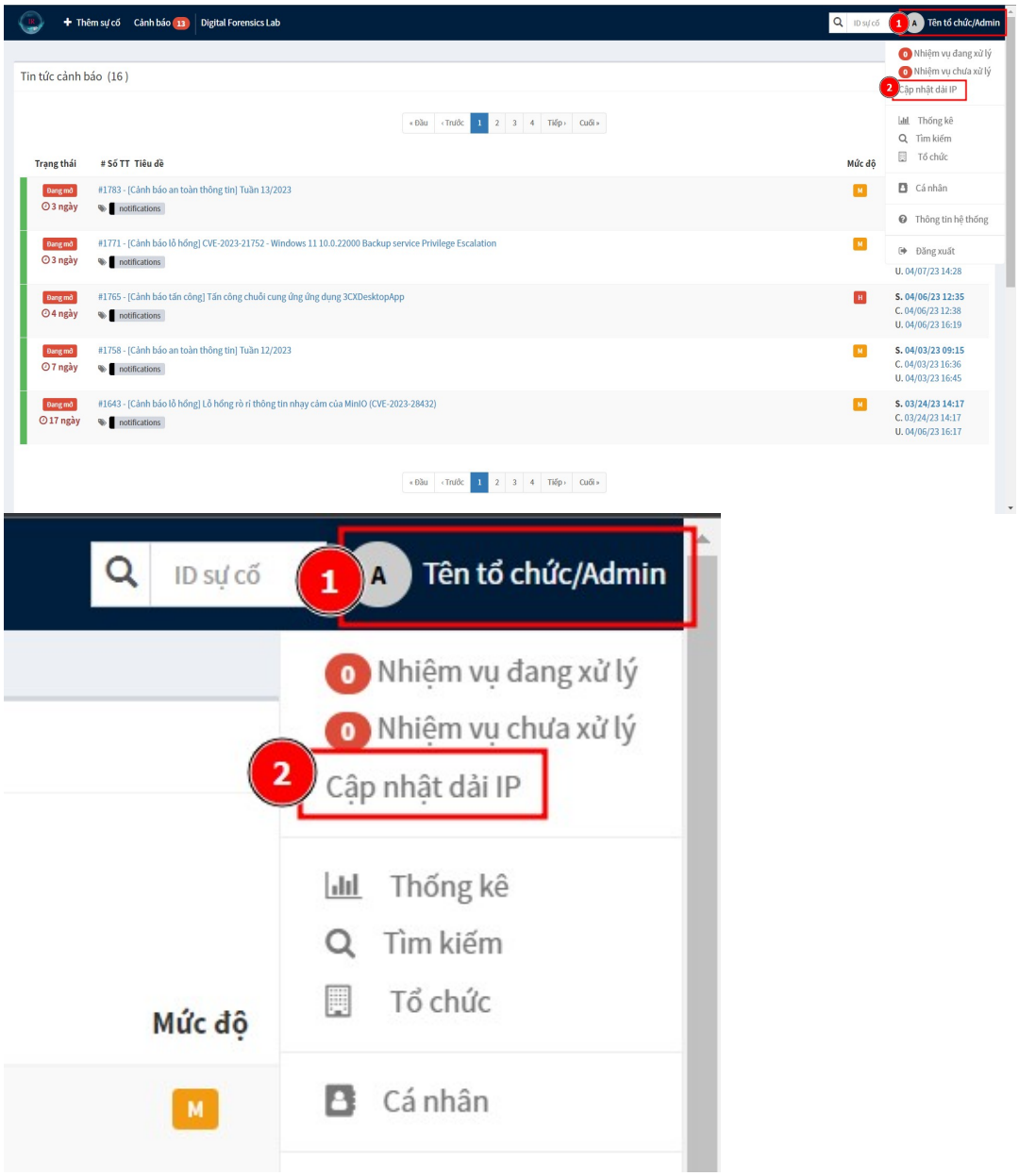
Khi đã tạo xong người dùng, quản trị viên có thể đặt mật khẩu bằng cách nhấp vào nút "Mật khẩu mới" trên hàng của người dùng tương ứng rồi nhấn ENTER hoặc nhấp vào nút tích màu xanh:



Hình 6: Màn hình đặt mật khẩu

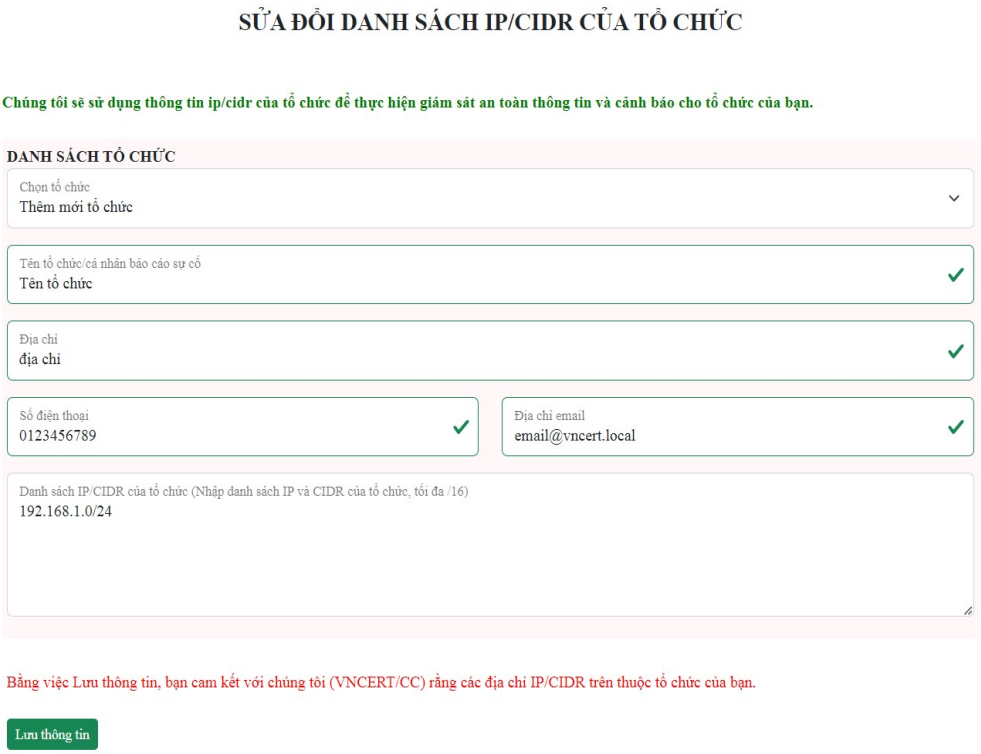
Cập nhật danh sách dải IP/CIDR

Khi đã tạo xong tài khoản của người dùng, quản trị viên có thể cập nhật dải IP/CIDR của tổ chức bằng cách click vào avatar, sau đó chọn mục "**Cập nhật dải IP**":



Hình 7: Màn hình "Cập nhật dải IP"

Với tổ chức lần đầu sử dụng IRLab, quản trị viên sẽ cần phải nhập thông tin về tổ chức:

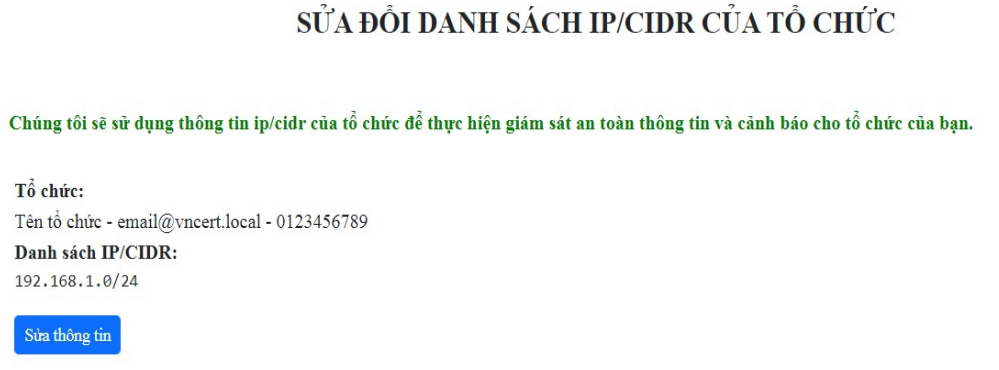


Hình 8: Màn hình nhập thông tin về tổ chức

Với trường IP/CIDR của tổ chức, các dữ liệu hợp lệ có thể nhập vào là:

- Địa chỉ IP Public của tổ chức (Ví dụ: 103.125.192.17)
- CIDR block của tổ chức (Ví dụ: 103.10.44.0/22)

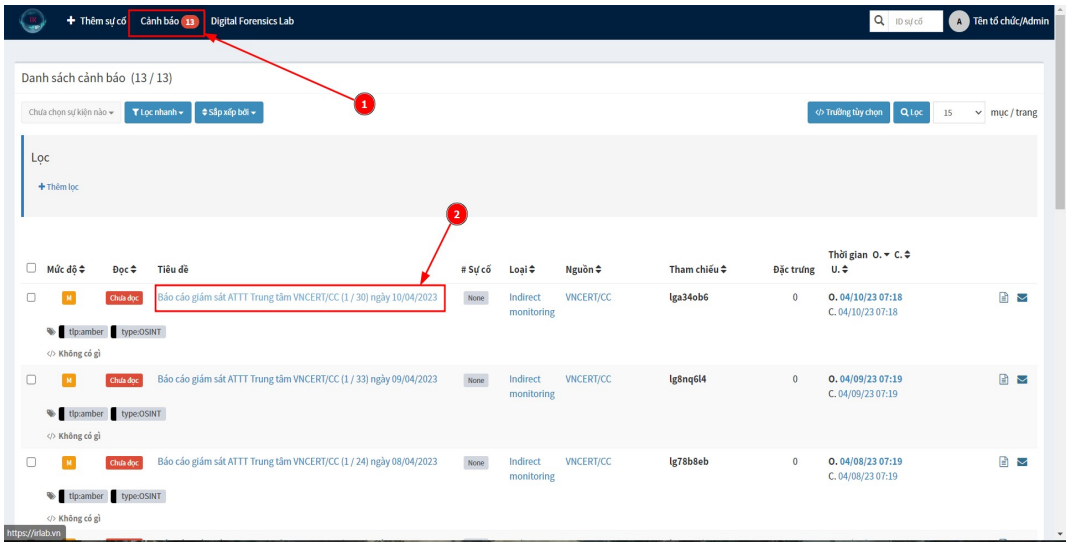
Sau khi lưu thông tin, quản trị viên có thể sửa đổi thông tin đã nhập bằng cách nhấn vào nút "Sửa thông tin":



Hình 9: Màn hình Sửa thông tin

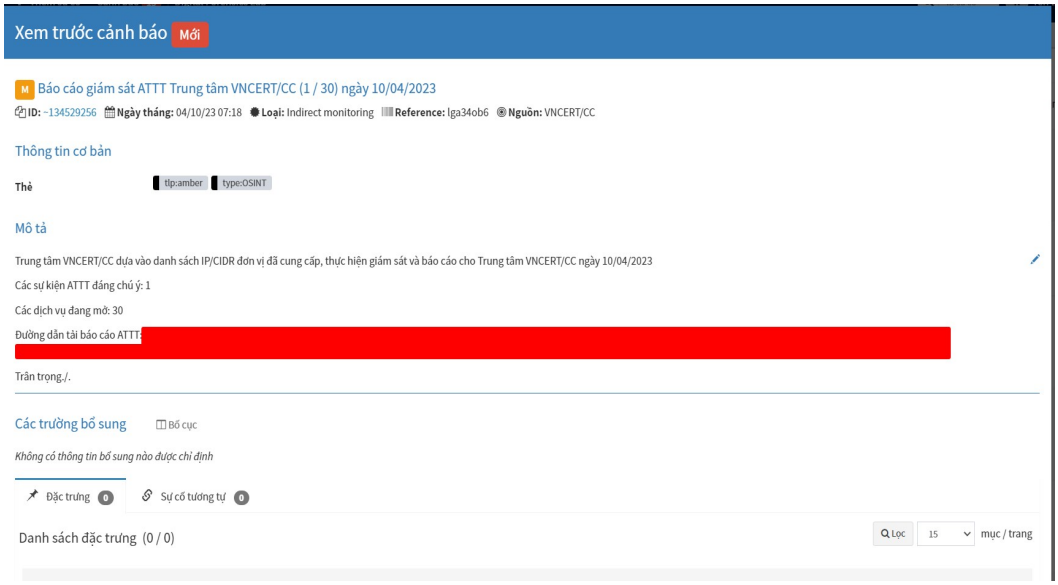
Xem nội dung báo cáo giám sát ATTT

Khi đã nhập xong danh sách IP/CIDR, quản trị viên có thể nhận báo cáo giám sát ATTT vào mỗi 7 giờ sáng:



Hình 10: Màn hình Nhận báo cáo giám sát ATTT

Quản trị viên có thể bấm vào tiêu đề để xem nội dung chi tiết của thông báo.



Hình 11: Màn hình Nhận/Tải báo cáo giám sát ATTT

Phụ lục 7
HƯỚNG DẪN SỬ DỤNG NỀN TẢNG HỖ TRỢ ĐIỀU TRA SỐ

1. Hướng dẫn đăng ký, kết nối Nền tảng DFLab

Các công cụ, tri thức, tình huống giả định đều được Trung tâm VNCERT/CC chia sẻ công khai thông qua website: https://df.irlab.vn/

Đối với các công cụ online, yêu cầu đăng ký để được hỗ trợ. Quy trình đăng ký như sau:

Bước 1: Các tổ chức, doanh nghiệp có nhu cầu sử dụng Công cụ phân tích online của Nền tảng DFLab, vui lòng gửi văn bản yêu cầu hỗ trợ, cung cấp tài khoản công cụ của Nền tảng DFLab đến Trung tâm VNCERT/CC. Thông tin trong văn bản bao gồm:

- Chỉ rõ công cụ yêu cầu hỗ trợ, cung cấp tài khoản.

- Mục đích sử dụng công cụ.

- Phạm vi dự kiến áp dụng công cụ trong hoạt động chuyên môn của tổ chức.

Bước 2: Trung tâm VNCERT/CC sẽ xác nhận thông tin và gửi thông tin phản hồi cho đầu mối đăng ký của tổ chức.

2. Hướng dẫn sử dụng Nền tảng DFLab

Các thành phần của DFLab

- Sổ tay ứng cứu sự cố
- Bộ công cụ hỗ trợ phân tích
- Hệ thống hỗ trợ phân tích
- Tình huống giả định

2.1. Sổ tay ứng cứu sự cố

Tổng quan

Sổ tay ứng cứu sự cố hướng dẫn, đưa ra các bước giải quyết các sự cố trong công việc hoặc tình huống khẩn cấp. Sổ tay bao gồm các thông tin, cách thực hiện các bước, các quy trình xử lý sự cố, các thông tin liên quan đến các nguồn lực và thiết bị ứng cứu. Sổ tay ứng cứu sự cố giúp chuyên gia, cán bộ kỹ thuật có thể nhanh chóng đưa ra các quyết định, hành động đúng cách, giảm thiểu thiệt hại và đảm bảo an toàn trong tình huống khẩn cấp.

Sổ tay ứng cứu sự cố mô tả quá trình cần thiết để quản lý các sự cố trên không gian mạng, cùng với các phản hồi và cách giải quyết để ngăn chặn hoặc hạn chế thiệt hại có thể gây ra. Việc áp dụng sổ tay sẽ giúp giảm phạm vi, tác động và mức độ ảnh hưởng của sự cố tới hệ thống CNTT và tổ chức.

Mỗi sổ tay sẽ bao gồm quy trình ứng cứu sự cố chung và các giai đoạn thực hiện ứng cứu sự cố, cụ thể:

- Giai đoạn 1: Chuẩn bị thông tin về các tài nguyên cần thiết, đảm bảo tính sẵn sàng.

- Giai đoạn 2: Xác định phạm vi của cảnh báo bảo mật, xác minh sự cố và mức độ nghiêm trọng.

- Giai đoạn 3: Điều tra chi tiết về sự cố, đảm bảo tất cả các thông tin được ghi nhận, xác định phạm vi của sự cố.

- Giai đoạn 4: Ngăn chặn và khắc phục, giảm thiểu rủi do gây ra từ sự cố.

- Giai đoạn 5: Đánh giá cuối cùng về sự cố, khôi phục hoạt động của hệ thống.

- Giai đoạn 6: Đóng hồ sơ.

Danh sách các sổ tay

- Sổ tay ứng cứu sự cố giả mạo (Phishing)

- Sổ tay ứng cứu sự cố mã độc (Malware)

2.2. Bộ công cụ

Tổng quan

DFLab giới thiệu, hướng dẫn sử dụng các công cụ mã nguồn mở, miễn phí và các công cụ do Trung tâm VNCERT/CC tự phát triển, hỗ trợ việc ứng cứu, điều tra sự cố. Mỗi công cụ được hướng dẫn với các mục sau: Giới thiệu công cụ, các chức năng chính và hướng dẫn sử dụng công cụ.

Bộ công cụ này giúp các chuyên gia phát hiện các bằng chứng, dấu hiệu của sự cố, lỗ hổng bảo mật, xác định nguyên nhân của các cuộc tấn công, giúp ứng phó và giải quyết các sự cố nhanh chóng và hiệu quả.

Một số công cụ điển hình:

- Thor Lite (Nextron Systems)

- Hayabusa (Yamato-Security)

- Autospy (The Sleuth Kit®)

- Timeline Explorer (Eric Zimmerman)

Danh sách các công cụ

- Công cụ do VNCERT phát triển
- Công cụ điều tra nhật ký sự kiện
- Công cu săn tìm mối đe doa
- Công cụ điều tra phương tiện lưu trữ
- Công cu điều tra thiết bi di đông
- Công cụ điều tra dữ liệu bộ nhớ
- Công cu điều tra mang

2.3. Hệ thống hỗ trợ ứng cứu, phân tích

DFLab cung cấp sẵn sàng các công cụ online sử dụng để phân tích và tra cứu nhật ký, phân tích hành vi mã độc, phân tích nhật ký theo thời gian,... để trợ giúp và rút ngắn thời gian ứng cứu sự cố.

Một số công cụ online được cung cấp như:

- Công cụ phân tích và tra cứu nhật ký
- Công cu phân tích nhật ký theo thời gian
- Công cụ hỗ trợ ứng cứu sự cố tập trung

(Vui lòng liên hệ với Trung tâm VNCERT/CC để truy cập và sử dụng các công cụ này)

2.4. Tình huống luyện tập

Tổng quan

Tình huống huấn luyện của DFLab được xây dựng trên mô hình mạng mô phỏng một doanh nghiệp vừa và nhỏ, đầy đủ các thành phần cơ bản, bao gồm: Vùng mạng server, Vùng mạng người dùng, Vùng mạng tấn công,...

Các tình huống của DFLab được xây dựng dựa trên việc mô phỏng các cuộc tấn công mạng nhắm vào nhiều thành phần khác nhau trong hệ thống mạng, thu thập các nhật ký, bằng chứng để người phân tích rà soát, tìm kiếm các dấu hiệu, hành động của kẻ tấn công. Mỗi tình huống bao gồm các mục: Bối cảnh, Câu hỏi, Tệp đính kèm.

Đội ngũ ứng cứu, điều tra sự cố, các chuyên gia, học viên, sinh viên là người chơi (hoặc đội chơi) truy cập vào từng tình huống đã xây dựng. Dựa vào

bối cảnh và các tệp đính kèm, các chuyên gia thực hiện phân tích, tìm kiếm dấu hiệu, bằng chứng của kẻ tấn công để lại trên nhật ký, qua đó trả lời được các câu hỏi đặt ra.

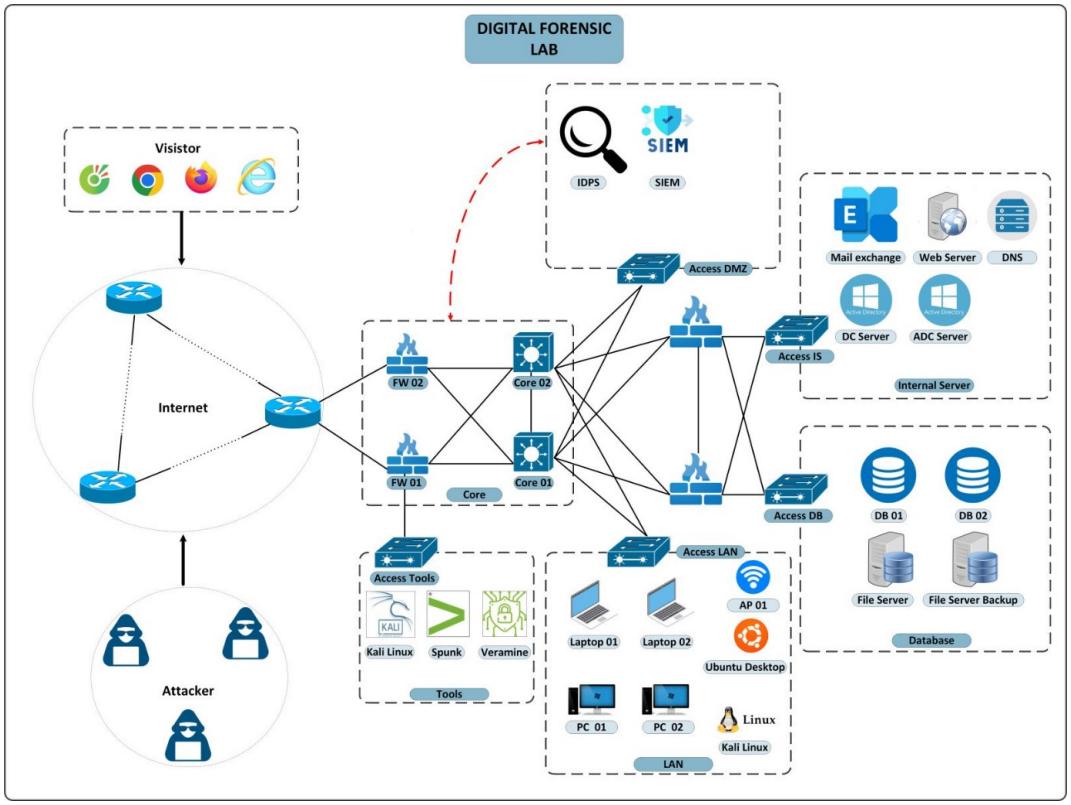
Sau khi trả lời được các câu hỏi, người chơi sẽ viết 01 báo cáo sự cố (tệp pdf hoặc docx, pptx,...) gửi cho Trung tâm VNCERT/CC, các chuyên gia sẽ xem xét tổng thể quá trình ứng cứu, điều tra sự cố, từ đó đưa ra điểm số phù hợp.

Các đội chơi có thành tích điểm số cao sẽ được vinh danh trên hệ thống xếp hạng và top 3 sẽ nhận được các phần quà đến từ Trung tâm VNCERT/CC.

Mô hình mạng

DFLab xây dựng một chuỗi kịch bản tấn công sát với thực tế và đưa ra các mẫu bằng chứng, tệp nhật ký,... cho các chuyên gia ứng cứu, điều tra, phân tích sự cố giả định.

Sự cố được giả định tại một Công ty có tên DFCorp có trụ sở tại Việt Nam. Công ty có tên miền dfcorp.com và sử dụng các máy chủ, được thiết kế và lắp đặt, kết nối theo sơ đồ sau:



Hình 1: Sơ đồ kết nối giả định của Công ty DFCorp (DFCorp Network)

Danh sách các dải mạng:

- DMZ: 10.0.9.0/24

- WZ: 10.0.8.0/24

- USERLAN: 10.0.10.0/24

Danh sách các thiết bị tham gia hệ thống mạng:

- Máy chủ ADDS (WZ): 10.0.8.2 cài đặt Windows Server 2019

- Máy chủ Database (WZ): 10.0.8.5 cài đặt

- Máy chủ MS Exchange (DMZ): 10.0.9.3 cài đặt Window Server 2019 và MS Exchange 2019

- Máy chủ IIS (DMZ): 10.0.9.4 cài đặt Windows Server 2019

- Máy chủ Firewall: 10.10.2.136 cài đặt pfSense

Lưu ý:

- Các nhân viên tham gia với dải mạng USERLAN

- Máy chủ IDS tham gia dải mạng USERLAN

- Các máy chủ MS Exchange và IIS được NAT ra ngoài mạng internet và được proxy thông qua haproxy đã được bật header x-forwarded-for.

Danh sách các tình huống

- Tình huống 1: Tấn công đào tiền ảo

- Tình huống 2: Tấn công mã hóa máy ảo

- Tình huống 3: Tấn công vào máy chủ web

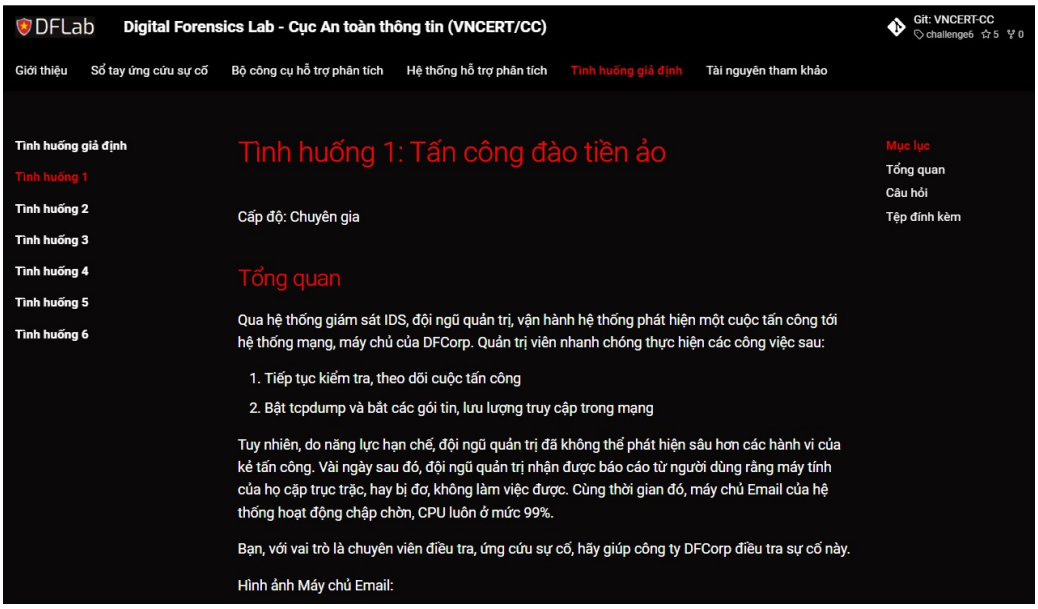
- Tình huống 4: Tấn công chiếm quyền trong môi trường domain

- Tình huống 5: Tình huống điều tra phân tích sự cố mail outlook

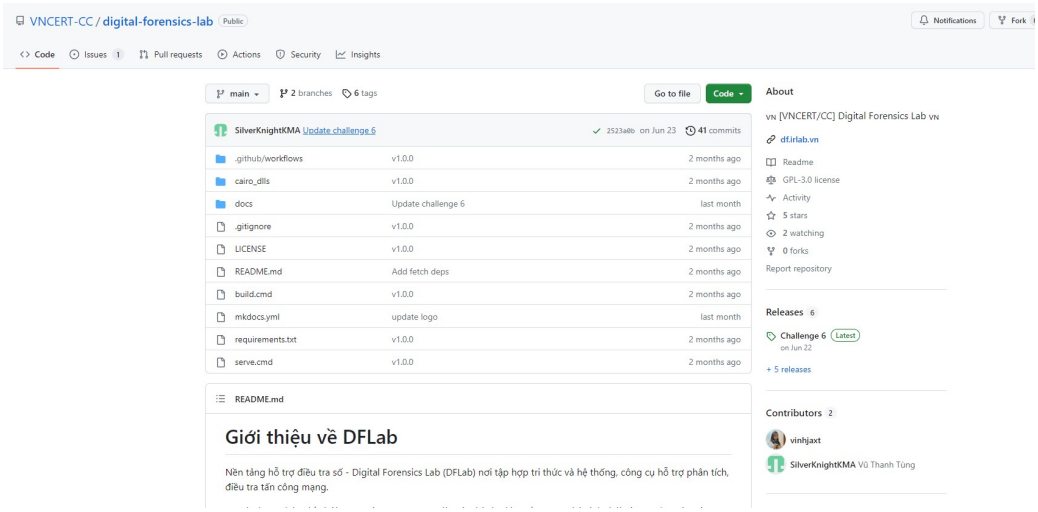
- Tình huống 6: Tình huống điều tra tấn công chuyển hướng website

Cách giải các tình huống luyện tập

Để giải các tình huống, người dùng cần truy cập vào trang chi tiết của từng sự cố, hoặc trang github của DFLab:



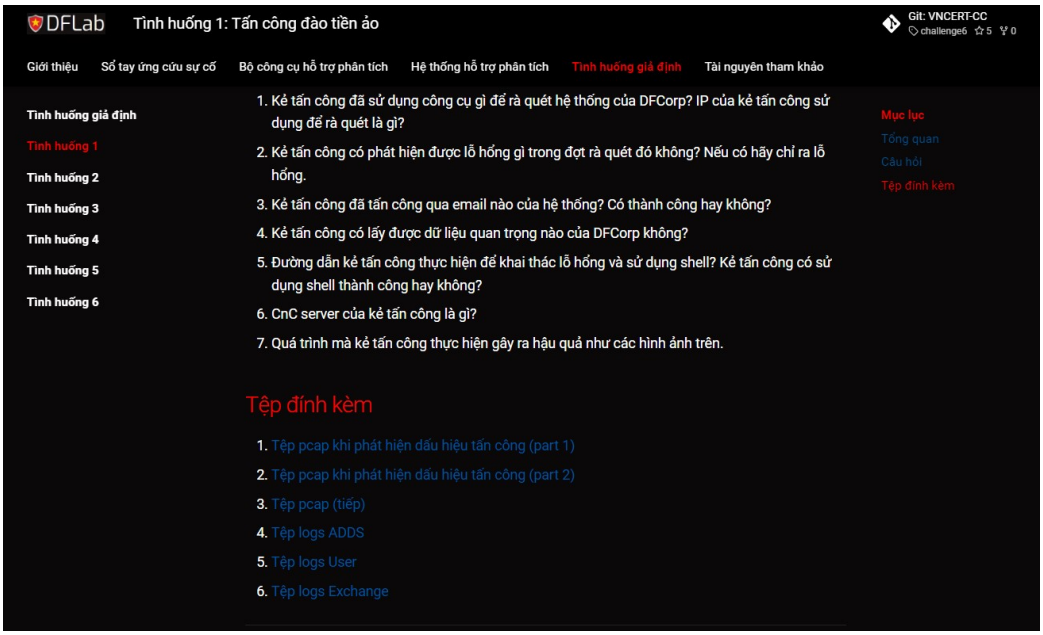
Hình 2: Chi tiết tình huống 1



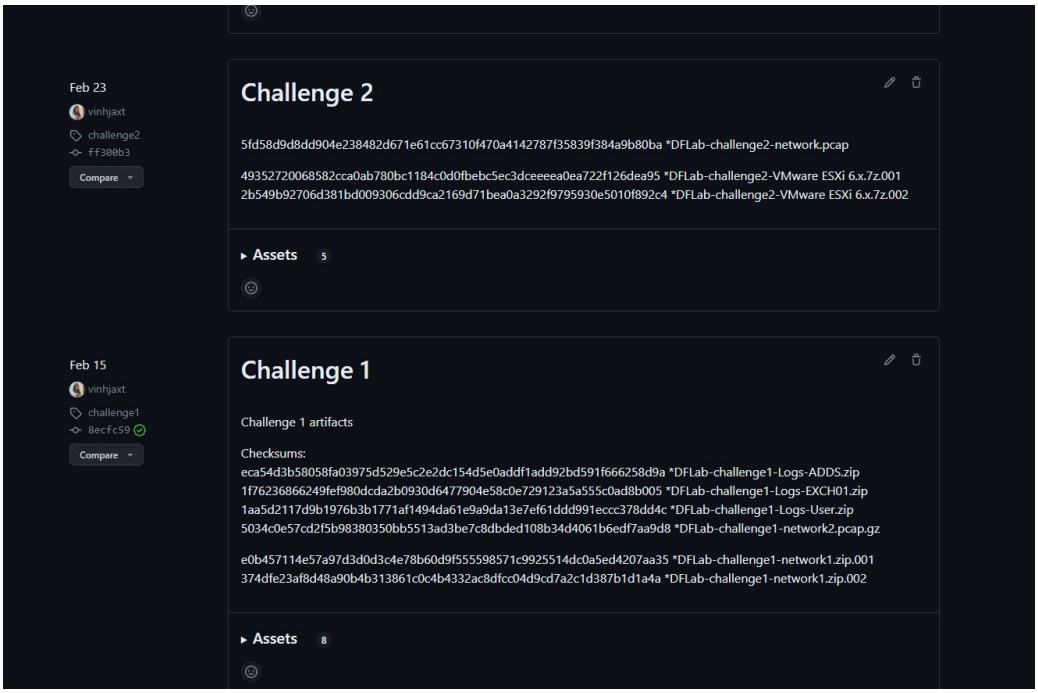
Hình 3: Trang github của DFLab

Đầu tiên, người chơi cần đọc nội dung của mục tổng quan để nắm được bối cảnh của tình huống, từ đó xác định hướng điều tra sự cố phù hợp, kết hợp với sơ đồ, hạ tầng mạng và các công cụ đã được cung cấp để tiến hành điều tra tình huống.

Người chơi có thể tải xuống các tập tin đính kèm ở cuối trang chi tiết hoặc mục release ở trang github:

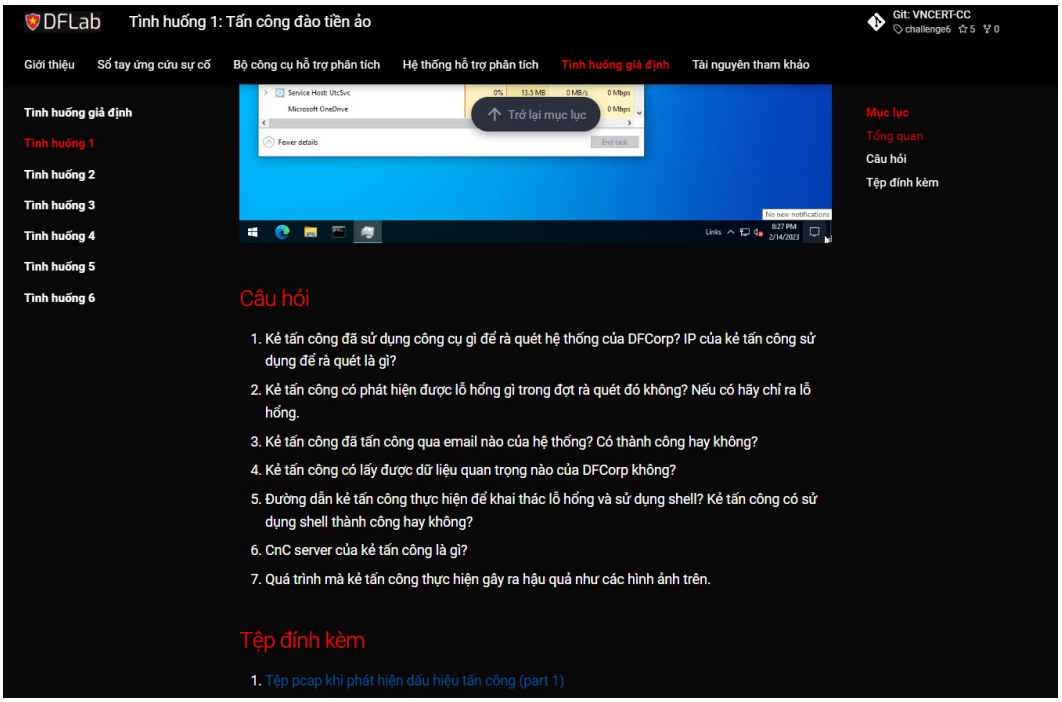


Hình 4: Tập tin đính kèm tại trang chi tiết tình huống



Hình 5: Tập tin đính kèm tại release trên github của nền tảng

Sau khi tải xuống, người chơi cần sử dụng các phần mềm giải nén, mở tập tin ảnh chứa các chứng cứ đã được thu thập, kết hợp các công cụ và kỹ năng để giải quyết tình huống và trả lời các câu hỏi được nêu ra ở mục câu hỏi:



Hình 6: Các câu hỏi của tình huống 1

Sau khi có được câu trả lời cho các câu hỏi thì người chơi sẽ viết một báo cáo sự cố gửi cho Trung tâm VNCERT/CC, đội ngũ chuyên gia của chúng tôi sẽ đánh giá báo cáo dựa trên các tiêu chí sau:

- Khả năng ghi nhận các hoạt động dò quét, thăm dò hệ thống.

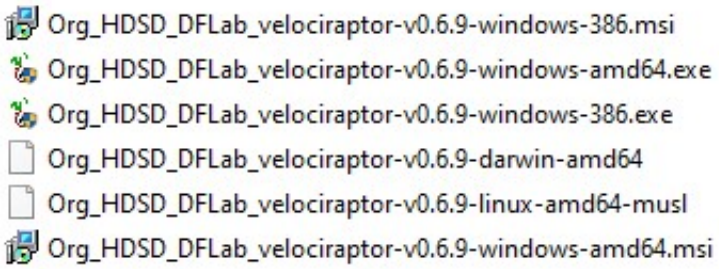
- Khả năng ghi nhận các tải trọng liên quan đến hoạt động dò quét, khai thác lỗ hổng.

- Khả năng phân tích tấn công để đưa ra dấu hiệu nhận diện, từ đó đưa ra phương án phản ứng và khắc phục sự cố.

Các đội chơi có thành tích điểm số cao sẽ được vinh danh trên hệ thống xếp hạng của DFLab và top 3 sẽ nhận được các phần quà đến từ VNCERT/CC.

2.5. Hướng dẫn sử dụng Công cụ hỗ trợ ứng cứu sự cố từ xa (VRX)

Khi đăng nhập lần đầu tiên, quản trị viên cần đăng nhập trên trang: https://vrx.irlab.vn/ bằng thông tin đăng nhập, và tải các công cụ đã được cung cấp.



Hình 7: Các công cụ được cung cấp trên https://vrx.irlab.vn/

Hệ thống hỗ trợ điều tra, ứng cứu sự cố nhanh trên các hệ điều hành sau:

- Windows 7 trở lên.

- Các hệ điều hành Linux sử dụng thư viện MUSL(x64) và MacOS.

Hệ thống sử dụng các agent được gọi là "máy trạm". Máy trạm kết nối với máy chủ và chờ các lệnh điều khiển, sau đó chạy câu lệnh và trả kết quả về máy chủ.

Có một số cách để chạy agent, tùy thuộc vào nhu cầu của quản trị hệ thống:

- Chạy trực tiếp

- Cài đặt MSI

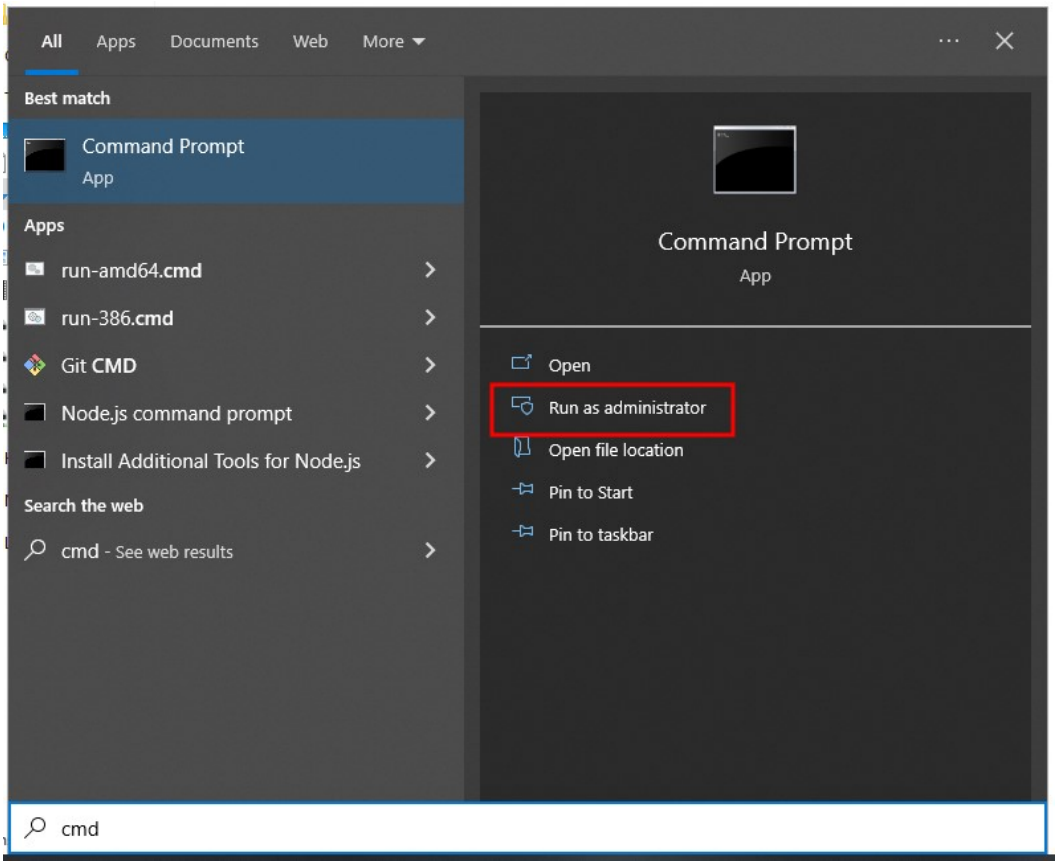
- Cài đặt agent dưới dạng dịch vụ

- Cài đặt agent trên Mac và Linux

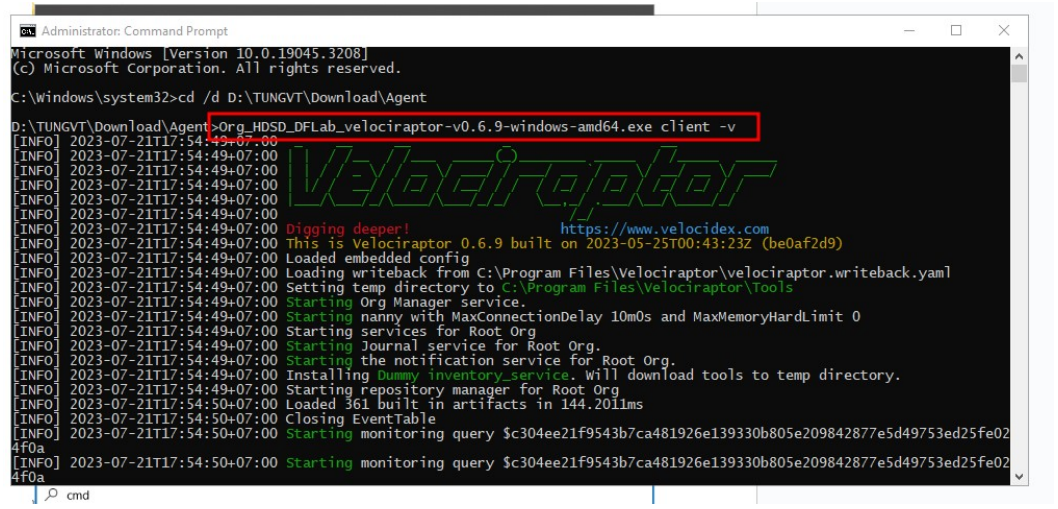
- Triển khai dưới dạng agentless

Chạy trực tiếp

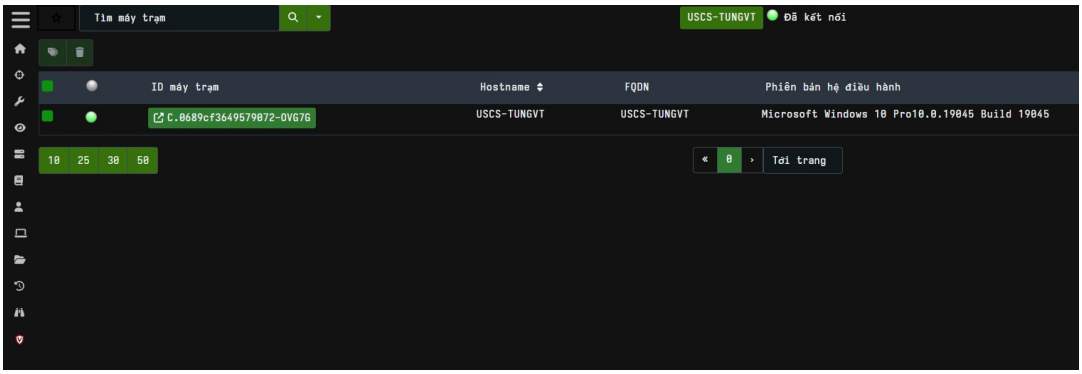
Phương pháp này phù hợp để kiểm tra kết nối của máy trạm tới máy chủ của hệ thống. Trong command shell với quyền admin, chỉ cần chạy tập tin .exe bằng cách sử dụng tham số "client -v":



Hình 8: Chạy command promt bằng quyền admin



Hình 9: Chạy công cụ agent với tham số "client -v"



Hình 10: Máy trạm đã được kết nối đến hệ thống

Lần đầu máy trạm kết nối nó sẽ đăng ký với máy chủ. Quá trình đăng ký yêu cầu máy trạm gửi về một số thông tin cơ bản về chính nó cho máy chủ.

Lưu ý rằng kiểu triển khai này sẽ hoạt động theo cùng một cách đối với tất cả các phiên bản của máy trạm (Windows, Linux hoặc Mac).

Cài đặt MSI

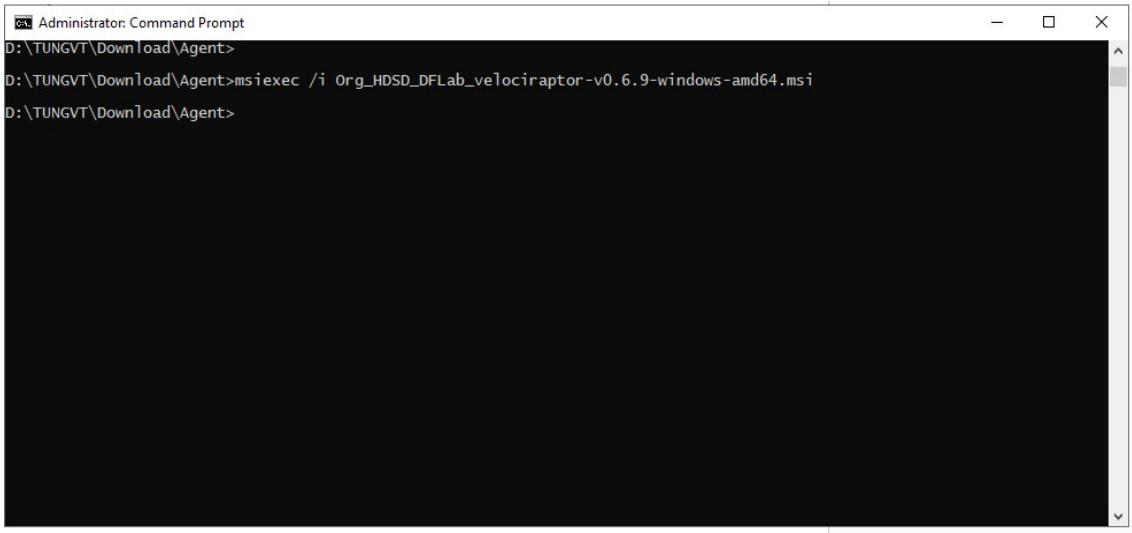
MSI là gói cài đặt Windows. Ưu điểm của phương pháp này so với chạy trực tiếp là hầu hết các công cụ quản trị hệ thống đều có thể được sử dụng để triển khai phần mềm trong định dạng MSI. Do đó, quản trị hệ thống có thể sử dụng SCCM hoặc Group Policy để cài đặt tập tin MSI.

Để biết thêm thông tin, vui lòng truy cập [How to use Group Policy to remotely install software in Windows Server 2008 and in Windows Server 2003]

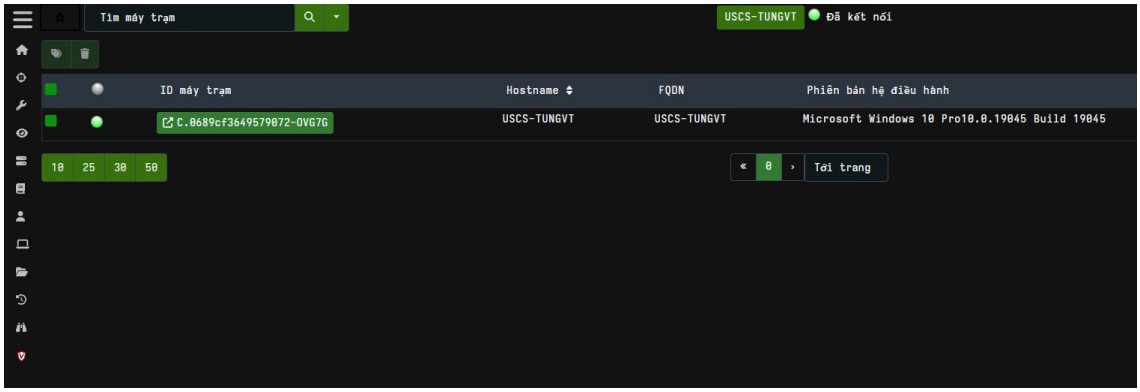
Cài đặt agent dưới dạng dịch vụ

Khi cài đặt bằng MSI, chỉ cần chạy câu lệnh sau với quyền administrator:

“msiexec /i agent.msi”



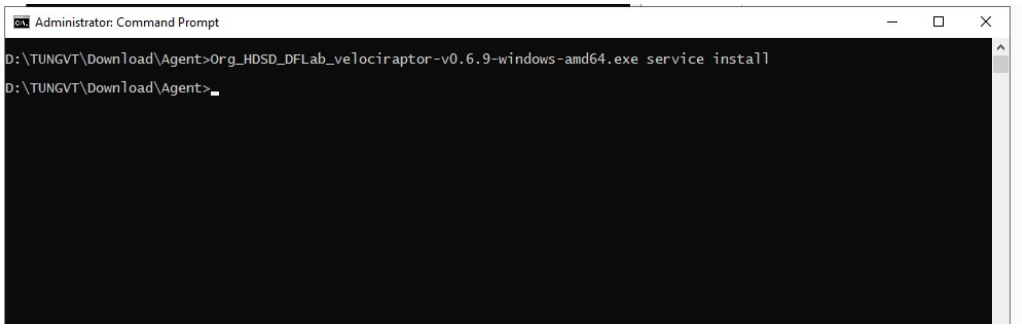
Hình 11: Cài đặt agent dưới dạng dịch vụ



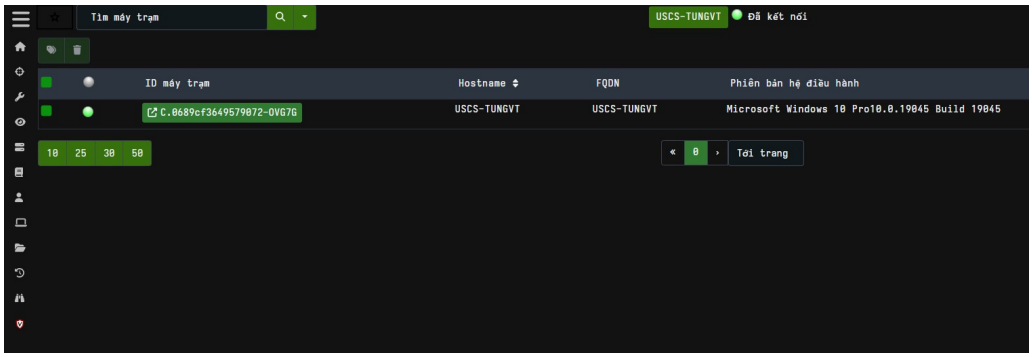
Hình 12: Máy trạm đã được kết nối đến hệ thống

Cũng có thể cài đặt tập tin exe cài đặt dưới dạng Windows Service thay vì sử dụng MSI. Triển khái dạng này không được khuyến nghị vì nó không sử dụng trình quản lý gói phù hợp và do đó không thể dễ dàng gỡ cài đặt hoặc nâng cấp.

Tuy nhiên, cách triển khai này có thể được thực hiện thông qua Group Policy scheduled tasks: “velociraptor.exe service install”.



Hình 13: Cài đặt dịch vụ bằng tập tin exe

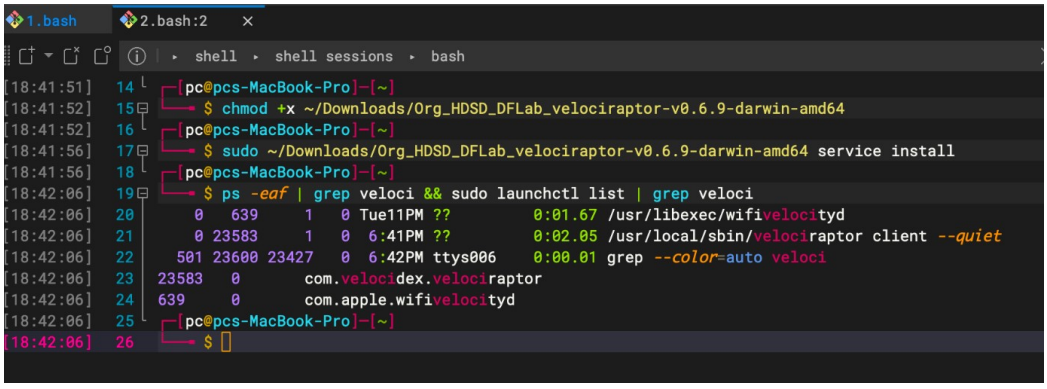


Hình 14: Máy trạm đã được kết nối đến hệ thống

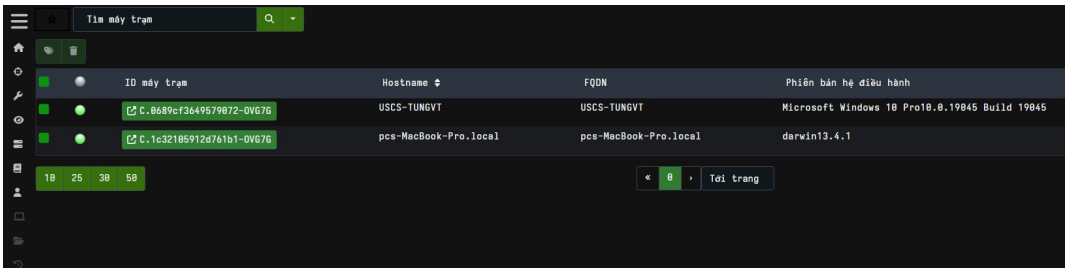
Cài đặt agent trên Mac

Tham số "service install" có thể được sử dụng để cài đặt Velociraptor trên máy trạm Mac. Câu lệnh cài đặt tập tin nhị phân và cấu hình tại "/usr/local/sbin"

Kiểm tra persistence với câu lệnh ps -eaf | grep veloci và sudo launchctl list | grep veloci



Hình 15: Cài đặt agent trên máy trạm Mac

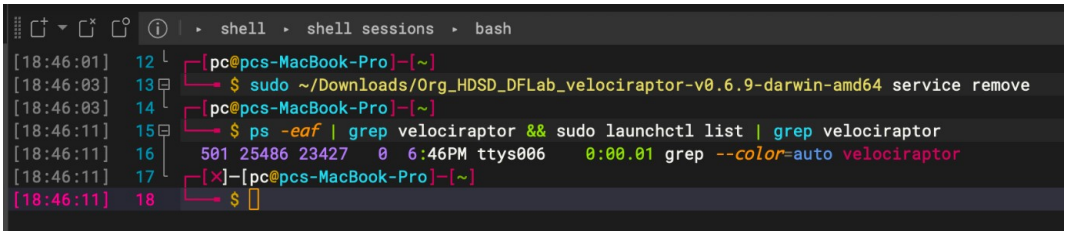


Hình 16: Máy trạm đã được kết nối đến hệ thống

Tham số "service remove" sử dụng để gỡ cài đặt:

/usr/local/sbin/velociraptor service remove

Hình 17: Gỡ cài đặt agent



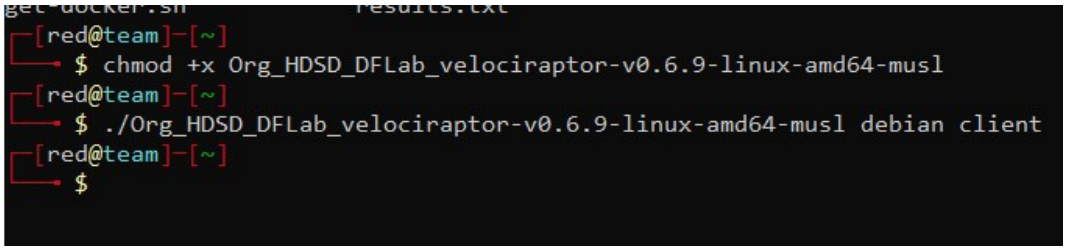
Hình 18: Xác minh không còn persistence

Cài đặt agent trên Linux

Có thể sử dụng công cụ dpkg (Debian) hoặc rpm (RedHat/CentOS) để cài đặt agent trên máy trạm Linux sau khi tạo gói thích hợp.

Debian Package

Tạo Debian package: "agent-linux-amd64 debian client"

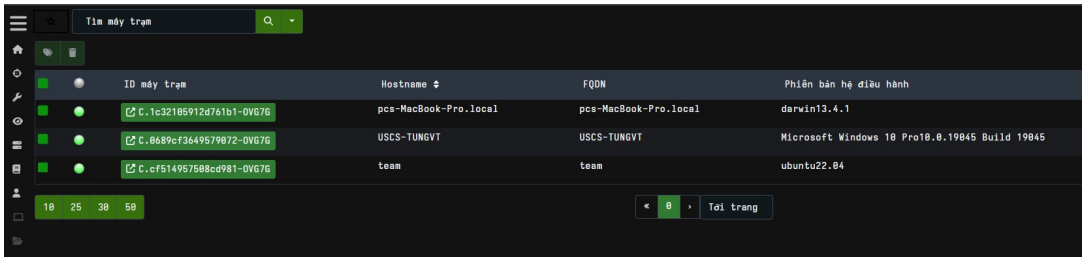


Hình 19: Tạo Debian package

Cài đặt package: "sudo dpkg -i agent.deb"

```
┌─[red@team]─[~]
└──╼ $ sudo dpkg -i velociraptor_0.6.9_client.deb
Selecting previously unselected package velociraptor-client.
(Reading database ... 116491 files and directories currently installed.)
Preparing to unpack velociraptor_0.6.9_client.deb ...
Unpacking velociraptor-client (0.6.9) ...
Setting up velociraptor-client (0.6.9) ...
Created symlink /etc/systemd/system/multi-user.target.wants/velociraptor_client.service → /etc/syste
md/system/velociraptor_client.service.
┌─[red@team]─[~]
└──╼ $
```

Hình 20: Cài đặt package



Hình 21: Máy trạm đã được kết nối đến hệ thống

Để gỡ cài đặt, quản trị viên có thể sử dụng câu lệnh sau: “sudo apt-get remove velociraptor-client”

```
┌─[red@team]─[~]
└──╼ $ sudo apt-get remove velociraptor-client
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libslirp0 slirp4netns
Use 'sudo apt autoremove' to remove them.
The following packages will be REMOVED:
  velociraptor-client
0 upgraded, 0 newly installed, 1 to remove and 103 not upgraded.
After this operation, 52.8 MB disk space will be freed.
Do you want to continue? [Y/n] y
(Reading database ... 116497 files and directories currently installed.)
Removing velociraptor-client (0.6.9) ...
Removed /etc/systemd/system/multi-user.target.wants/velociraptor_client.service.
dpkg: warning: while removing velociraptor-client, directory '/usr/local/bin' not empty so not remov
ed
Scanning processes...
Scanning candidates...
Scanning linux images...
```

Hình 22: Gỡ cài đặt agent

Red Hat Package

Về cơ bản quá trình tạo RPM package cho agent cũng tương tự với debian, chỉ cần thay thế tham số debian bằng rpm

Tạo RPM package trên OS có systemctl: “agent rpm client”

Tạo RPM package trên OS không có RPM và sử dụng GLIBC (Ví dụ CentOS6): “agent rpm client --use_sysv”

Cài đặt package: “sudo rpm -i agent.rpm”

Gỡ cài đặt package: “rpm -qa | grep -i velociraptor && sudo rpm -e velociraptor-x.x.x.X86_64”

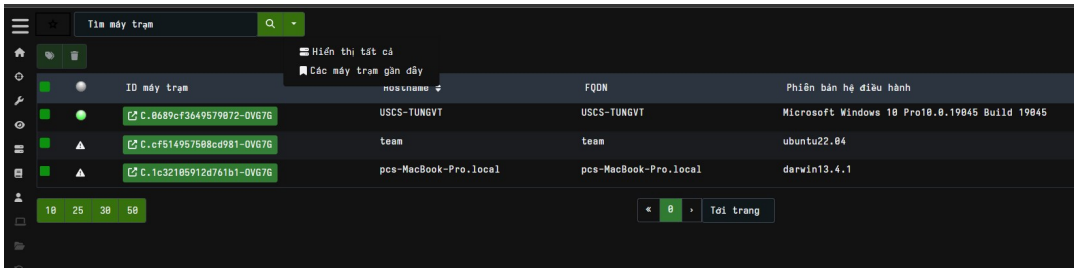
Kiểm tra máy trạm

Máy trạm là điểm cuối với agent chạy trên từng thiết bị. Vì agent duy trì kết nối liên tục với máy chủ nên mỗi máy trạm đều có thể nhận yêu cầu ngay lập tức để tiến hành hoạt động ứng cứu sự cố và săn tìm mối đe doạ.

Thông thường, quản trị hệ thống bắt đầu cuộc điều tra bằng cách tìm kiếm một máy trạm, chọn máy trạm đó và thu thập các dấu vết từ máy trạm bằng yêu cầu từ máy chủ đến agent.

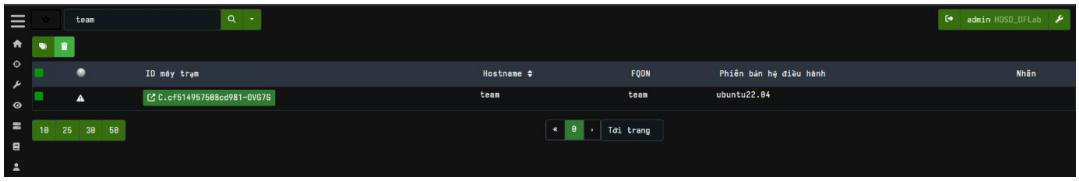
Tìm máy trạm

Để thực hiện yêu cầu với một máy trạm cụ thể, quản trị viên tìm kiếm máy trạm đó bằng thanh tìm kiếm ở phía trên giao diện quản trị. Nhấp vào biểu tượng Tìm kiếm hoặc “Hiển thị tất cả” để xem tất cả các máy trạm đã kết nối.



Hình 23: Tìm kiếm máy trạm

Lưu ý: Quản trị viên có thể tìm kiếm theo nhãn với “label:” hoặc “host:” để tìm kiếm hostname. Chức năng tìm kiếm sẽ trả về kết quả dưới dạng một bảng.



Hình 24: Kết quả tìm kiếm

Bảng kết quả bao gồm 6 cột:

1. Trạng thái trực tuyến của máy trạm được hiển thị dưới dạng biểu tượng màu. Dấu chấm màu xanh cho biết máy trạm hiện đang được kết nối với máy chủ, biểu tượng màu vàng cho biết máy trạm hiện không được kết nối nhưng đã được kết nối từ 15 phút đến 24 giờ trước. Biểu tượng màu đỏ cho biết rằng máy chủ đã không được nhìn thấy trong 24 giờ trở lên.

2. ID máy trạm. Mỗi máy trạm có một ID duy nhất bắt đầu bằng “C.”. ID máy trạm được coi là đặc điểm nhận dạng điểm cuối chính xác nhất.

3. Hostname của máy trạm.

4. FQDN của máy trạm.

5. Phiên bản hệ điều hành. Cột này cho biết liệu máy chủ có phải là máy Windows/Linux/MacOS hay không và phiên bản tương ứng của nó.

6. Bất kỳ nhãn nào được gán cho máy trạm.

Nhãn

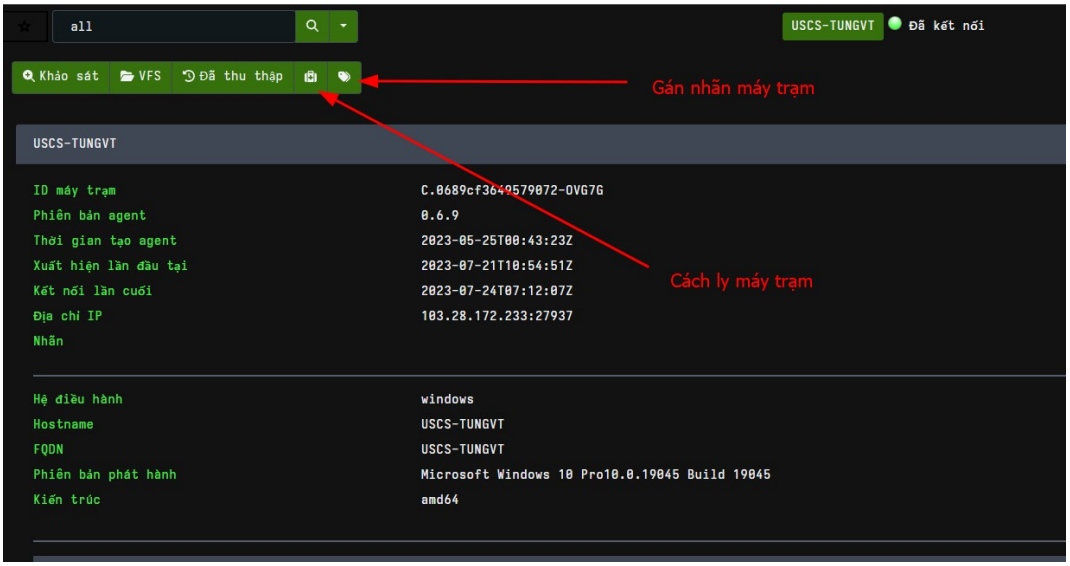
Máy trạm có thể có nhiều nhãn được gán. Một nhãn là chuỗi ký tự có liên quan đến máy trạm, được sử dụng để định danh một nhóm máy trạm. Quản trị viên có thể hạn chế săn tìm trong một hoặc nhiều nhãn để hạn chế thu thập thông tin hoặc truy cập máy trạm không cần thiết.

Để gán nhãn cho máy trạm, chọn máy trạm trên giao diện và bấm nút “Nhãn máy trạm”

Hình 25: Gán nhãn cho máy trạm

Thao tác với máy trạm

Nhấp vào bất kỳ máy trạm nào trong giao diện tìm kiếm để xem thông tin liên quan đến máy trạm đã chọn. Quản trị viên có thể kiểm tra công cụ đang xử lý máy trạm nào bằng hostname và lần cuối cùng máy chủ kết nối với nó:



Hình 26: Tổng quan máy trạm

Máy chủ sẽ yêu cầu một số thông tin cơ bản về máy trạm, bao gồm hostname, nhãn, địa chỉ IP và lần cuối kết nối trong lần đầu kết nối, trong giai đoạn "Khảo sát". Khảo sát thường chỉ được chạy khi máy trạm kết nối lần đầu, tuy nhiên quản trị viên có thể khảo sát bất kỳ lúc nào bằng cách nhấn vào biểu tượng "Khảo sát".

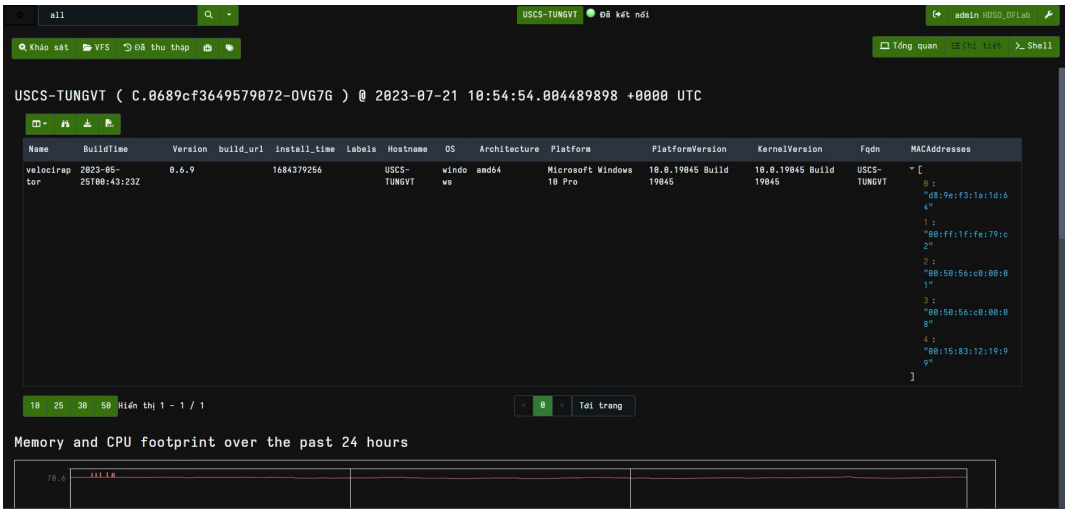
Cách ly máy trạm

Quản trị viên có thể cách ly máy trạm từ giao diện tổng quan. Việc cách ly một máy trạm sẽ cấu hình lại mạng của máy trạm để chỉ cho phép nó giao tiếp với máy chủ của công cụ ứng cứu sự cố từ xa. Điều này cho phép các chuyên gia tiếp tục điều tra máy trạm từ xa trong khi ngăn không cho nó thực hiện các kết nối mạng khác.

Máy khách bị cách ly sẽ có nhãn "Quarantine" để quản trị viên có thể tìm kiếm tất cả các máy trạm đã cách ly bằng tính năng tìm kiếm nhãn ở trên. Xóa nhãn cách ly khỏi máy chủ sẽ ngay lập tức hủy cách ly máy chủ.

Chi tiết

Chọn nút "Chi tiết" sẽ hiển thị thông tin tổng quan về máy trạm:

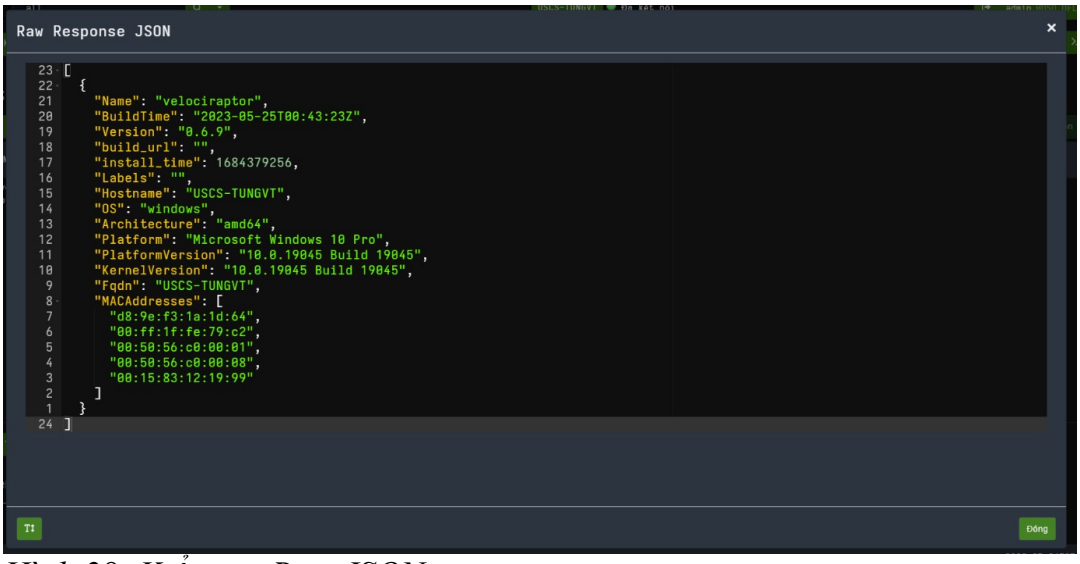


Hình 27: Chi tiết máy trạm

Các bảng sẽ có một số công cụ như có thể nhìn trong hình:

1. Bảng chọn cột: Cho phép người dùng ẩn/hiện cột. Tính năng này được sử dụng khi có quá nhiều cột và bảng chiếm quá nhiều diện tích hoặc một số cột thể hiện quá nhiều chi tiết.

2. Xem Raw JSON: Tất cả các yêu cầu từ máy chủ sẽ trả về kết quả dưới dạng một đối tượng JSON. Với các bảng phức tạp, có thể xem dưới dạng Raw JSON sẽ dễ để kiểm tra kết quả.

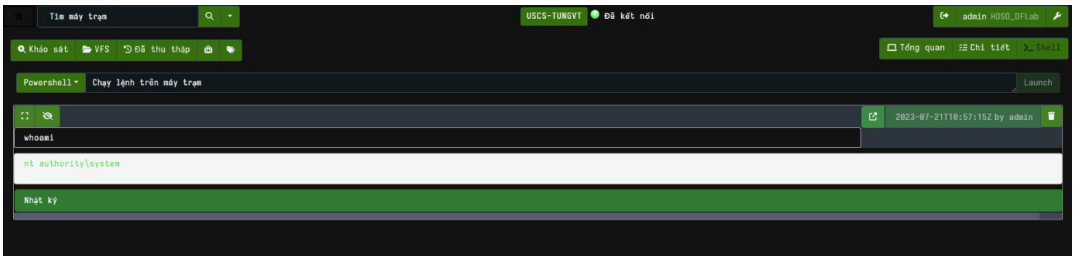


Hình 28: Kiểm tra Raw JSON

3. Xuất bảng dưới dạng CSV: Bấm vào nút Tải xuống CSV sẽ xuất các cột đang được hiển thị thành một tập tin CSV.

Thực thi lệnh từ xa

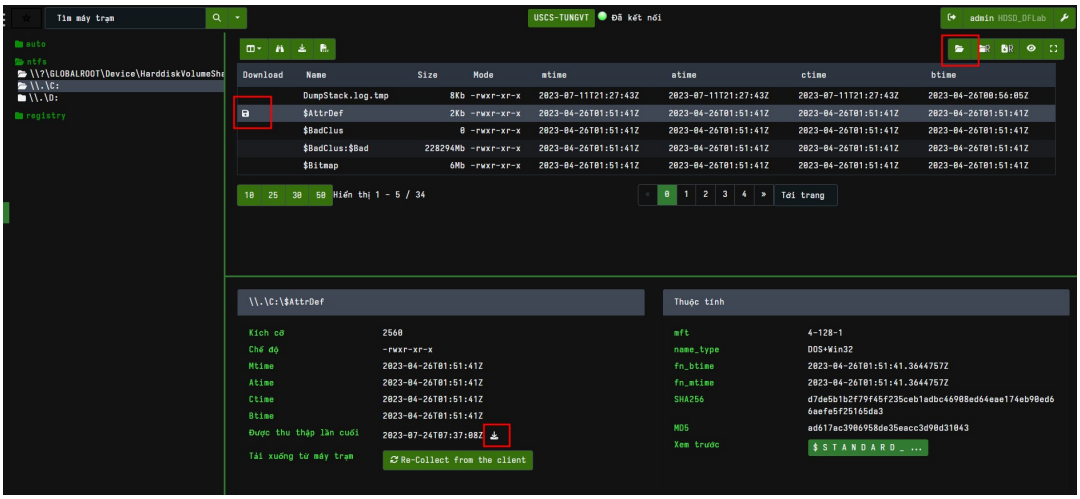
Quản trị viên nên thu thập dấu vết thông qua săn tìm hoặc chạy các dấu vết riêng biệt trên từng máy trạm. Tuy nhiên có một số lúc sẽ cần thực hiện câu lệnh trên máy trạm trong trường hợp ứng cứu sự cố.



Hình 29: Thực thi lệnh từ xa

VFS

Để kiểm tra tập tin trên máy trạm, quản trị viên có thể sử dụng tính năng Virtual Filesystem View (VFS). VFS là một bộ đệm lưu các tập tin của máy trạm trên máy chủ, cho phép người dùng điều tra tập tin trên máy trạm.



Hình 30: Giao diện VFS

VFS có chế độ xem dạng cây ở ngăn bên trái và danh sách tập tin ở ngăn bên phải. Chế độ xem dạng cây cho phép quản trị viên điều hướng qua hệ thống tệp, bắt đầu từ cấp cao nhất.

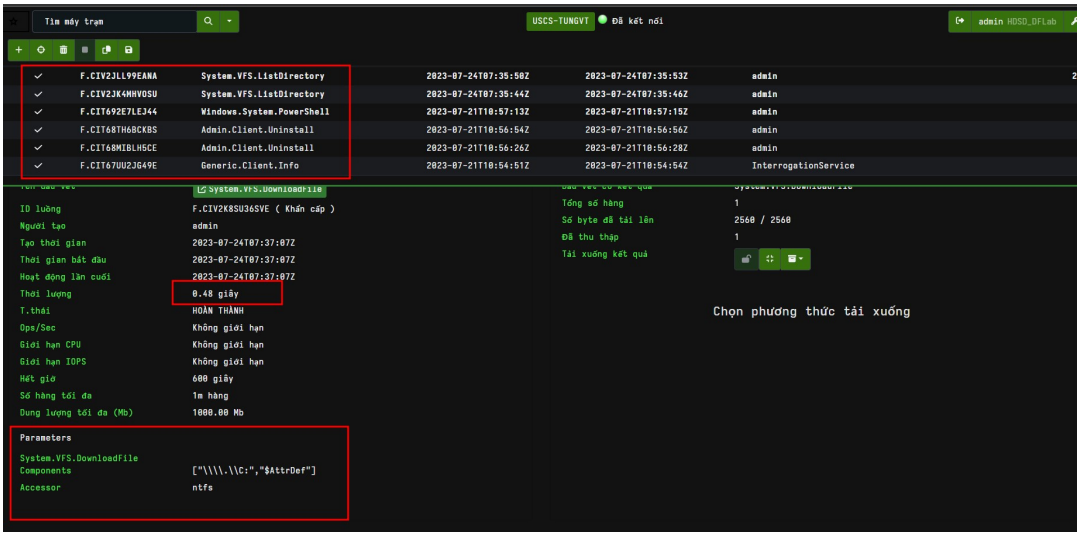
Khi mở một thư mục trong chế độ xem dạng cây chưa được đồng bộ hóa từ máy trạm, ngăn bên phải trống. Nhấp vào nút làm mới thư mục sẽ bắt đầu hoạt động liệt kê thư mục trên máy trạm và cung cấp cho máy trạm hiện đang được kết nối, sẽ làm mới chế độ xem VFS. Nhấp vào bất kỳ tệp nào trong danh sách thư mục, sẽ hiển thị thuộc tính ở ngăn dưới.

Người dùng có thể tải xuống tập tin / thư mục từ máy trạm. Sau khi một tệp được lưu từ điểm cuối, nó sẽ được lưu trữ trên máy chủ và quản trị viên có

thể xem nó trong VFS GUI. Tập tin cũng được đánh dấu bằng biểu tượng đĩa mềm. Người dùng có thể tải xuống tệp đã thu thập từ máy chủ bằng cách nhấp vào biểu tượng tải xuống. Người dùng có thể liệt kê toàn bộ danh sách tập tin / thư mục trên một địa chỉ nhất định bằng cách nhấn nút làm mới / tải xuống tất cả nội dung thư mục này.

Dấu vết

Bấm vào nút "Đã thu thập" trên giao diện tổng quan máy chủ để truy cập các dấu vết đã thu thập:



Hình 31: Các dấu vết đã thu thập

Trang này bao gồm 2 phần, phần trên hiển thị các dấu vết đã thu thập, phần dưới thể hiện thông tin chi tiết về dấu vết đang chọn. Mỗi dấu vết sẽ có một ID luồng riêng biệt để thể hiện danh sách các dấu vết đã được thu thập. Dấu vết là cách để người dùng yêu cầu máy trạm cung cấp các kết quả về máy chủ.

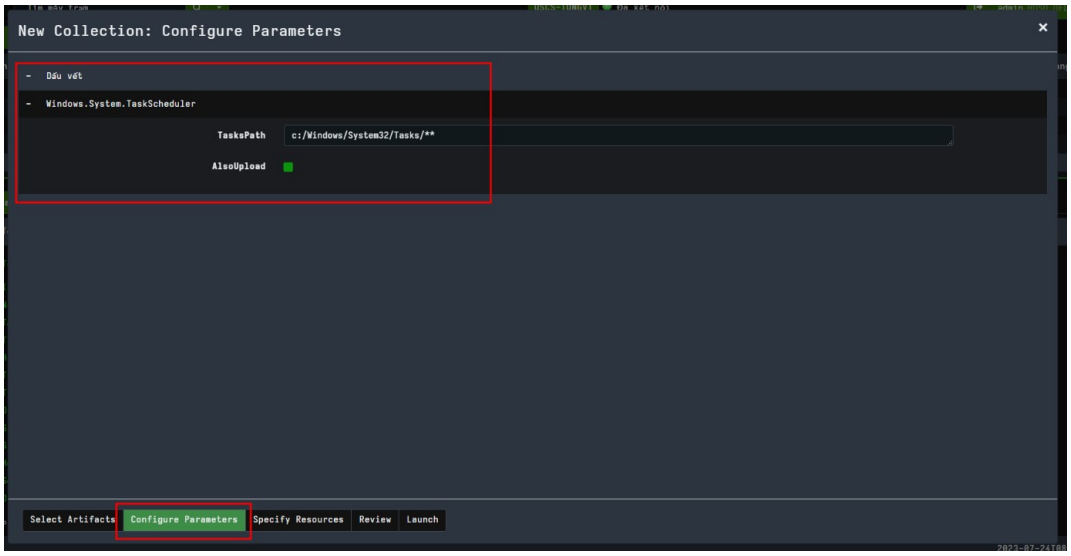
Ví dụ: Thu thập scheduled tasks từ máy trạm

Bắt đầu thu thập dấu vết bằng cách bấm vào nút "Danh sách mới". Giao diện thu thập dấu vết sẽ xuất hiện:

Hình 32: Giao diện thu thập dấu vết

Giao diện có nhiều bước để hướng dẫn người dùng thu thập dấu vết. Ở bước đầu, tìm kiếm tên dấu vết "Windows.System.TaskScheduler"

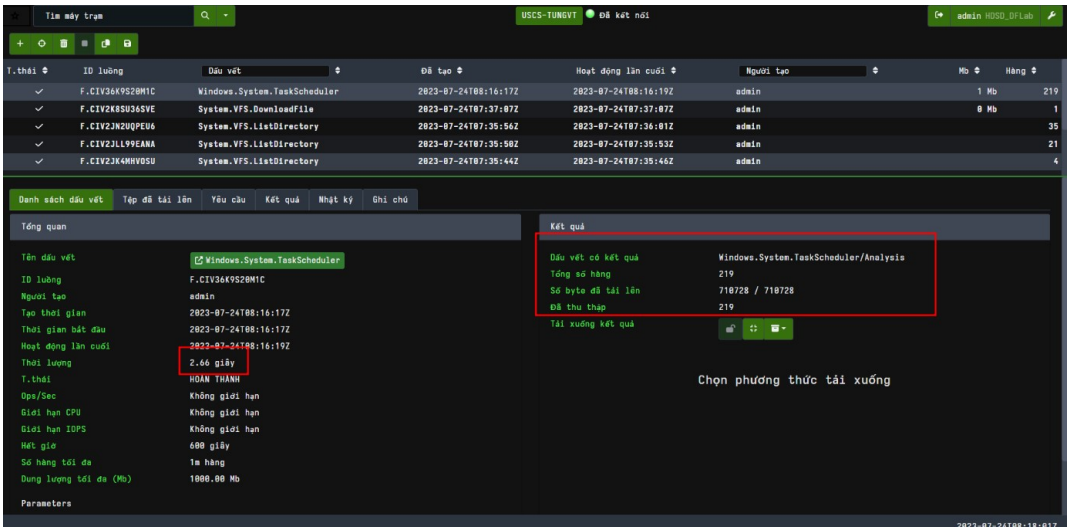
Bước tiếp theo cho phép chỉnh sửa tham số của dấu vết



Hình 33: Chỉnh sửa tham số dấu vết

Mỗi tham số sẽ có giá trị mặc định.

Sau khi điều chỉnh các tham số và tiến hành thu thập dấu vết, người dùng sẽ thấy kết quả hiển thị trên danh sách các dấu vết đã thu thập:

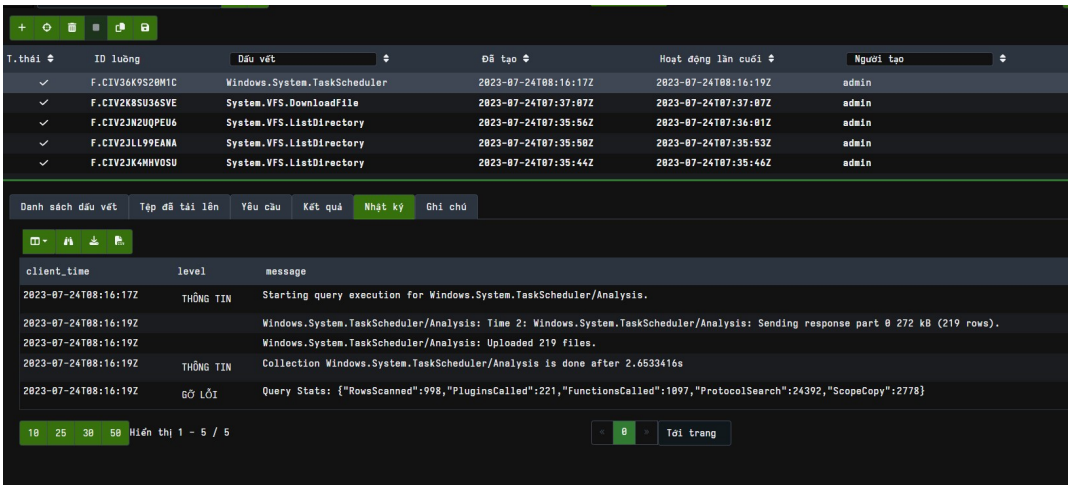


Hình 34: Kết quả của việc thu thập dấu vết

Người dùng có thể xem các thông tin chi tiết hơn tại các tab phía dưới:

Nhật ký

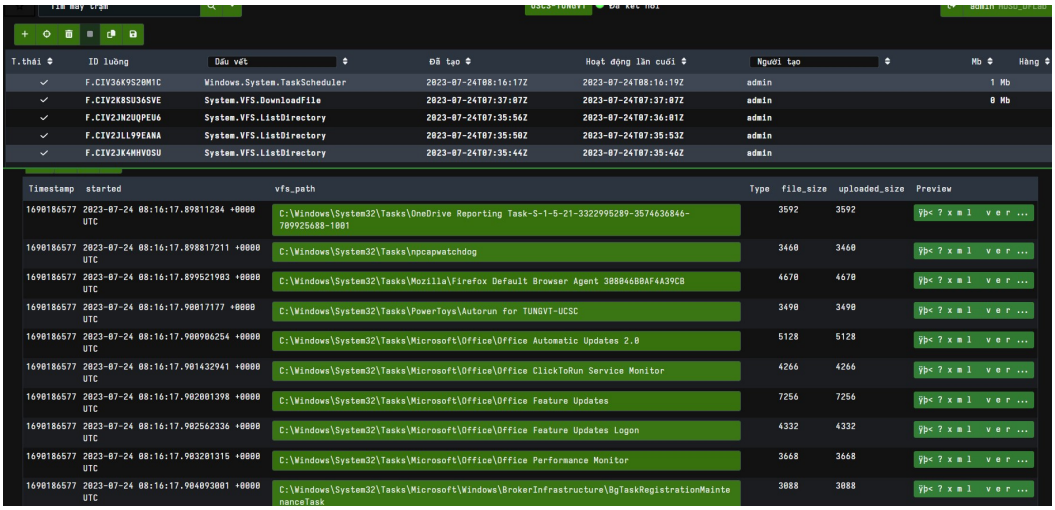
Các thông báo xuất hiện khi thực hiện thu thập dấu vết sẽ được thu thập từ máy trạm và gửi tại đây. Người dùng có thể kiểm tra yêu cầu đã được thực hiện như thế nào thông qua nhật ký



Hình 35: Nhật ký thu thập dấu vết

Tập tin tải lên

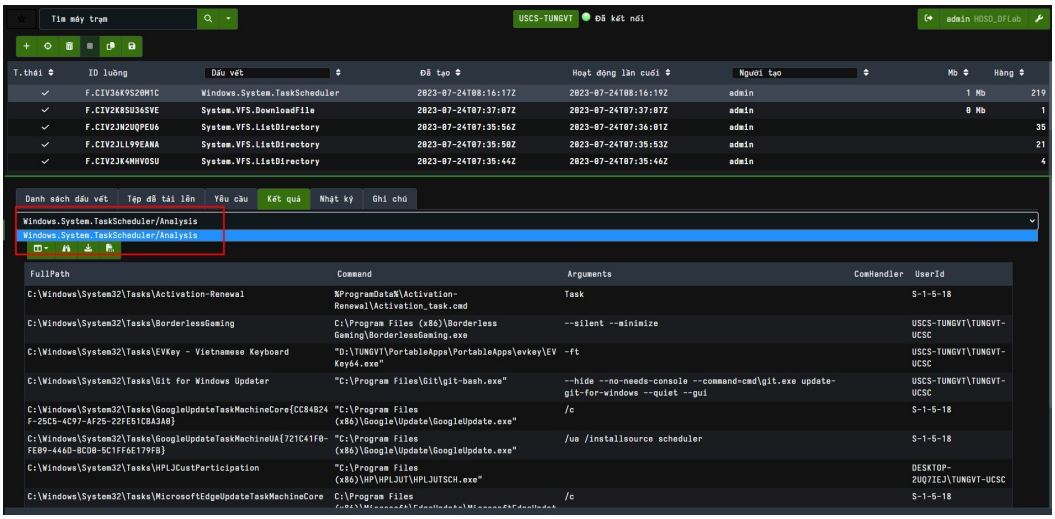
Các tập tin được tải lên máy chủ sẽ xuất hiện tại đây.



Hình 36: Các tập tin đã tải lên

Kết quả

Kết quả của yêu cầu thu thập dấu vết được hiển thị dưới dạng bảng. Một yêu cầu thu thập dấu vết có thể chứa nhiều dấu vết, người dùng có thể chọn dấu vết để xem bằng cách chọn menu thả xuống.



Hình 37: Dấu vết đã thu thập

Săn tìm

Với công cụ hỗ trợ ứng cứu từ xa, người dùng có thể thu thập các dấu vết giống nhau từ nhiều máy trạm sử dụng chức năng "Săn tìm". Chức năng săn tìm có thể làm được các việc sau:

- Giám sát các máy trạm ngắt kết nối bằng cách lên lịch săn tìm thu thập từ bất kỳ máy trạm nào có kết nối mạng trong một khoảng thời gian.
- Kiểm tra kết quả săn tìm trên tất cả các máy trạm dễ dàng.

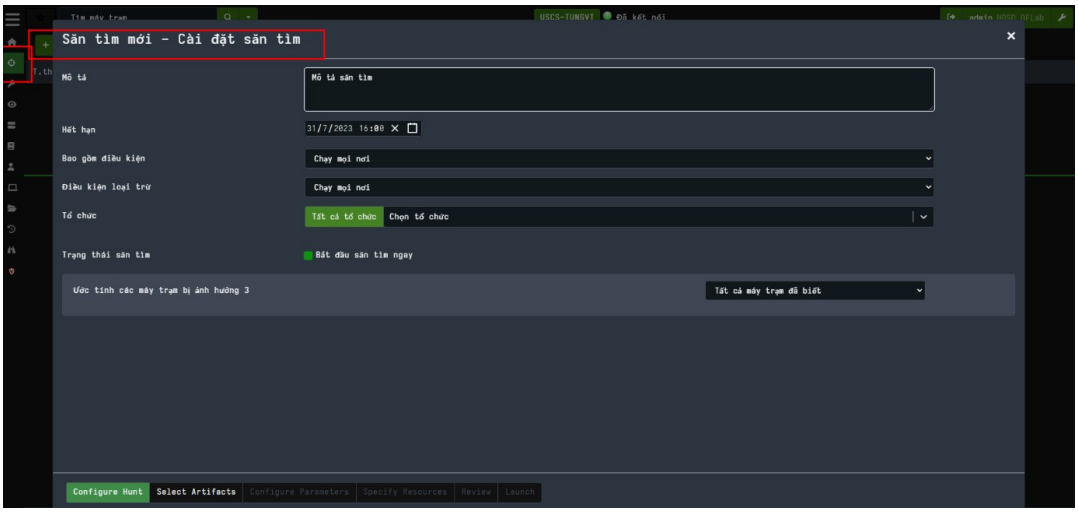
- Theo dõi máy trạm nào đã thực hiện thu thập dấu vết và không thu thập một dấu vết hai lần trên các máy trạm.

Một săn tìm là một tập hợp một hoặc nhiều dấu vết.

Quản lý săn tìm

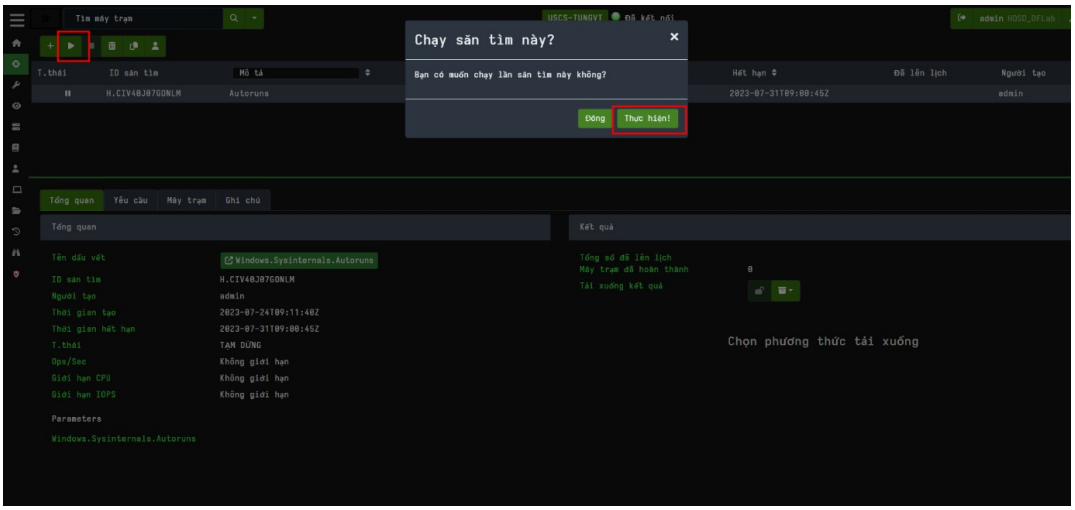
Quản lý săn tìm là giao diện chịu trách nhiệm quản lý, lên lịch và giám sát các tiến trình thu thập bên trong săn tìm.

Để lên lịch một săn tìm mới, chọn "Quán lý săn tìm", sau đó chọn săn tìm mới:



Hình 38: Thêm săn tìm mới

Người dùng có thể thêm mô tả, hẹn ngày hết hạn, chọn các máy trạm có nhãn nhất định săn tìm:



Hình 39: Chọn săn tìm

Phụ lục 8
THIẾT LẬP VÀ QUẢN LÝ VẬN HÀNH HỆ THỐNG GIÁM SÁT

1. Hướng dẫn chung

Để thiết lập hệ thống giám sát, trước hết cơ quan, tổ chức phải xác định phạm vi và đối tượng và các yêu cầu đối với hệ thống giám sát làm cơ sở để lựa chọn giải pháp, công nghệ và năng lực xử lý phù hợp.

Giải pháp giám sát cần triển khai kết hợp nhiều lớp giám sát khác nhau một cách đồng bộ, thống nhất tối thiểu bao gồm: Giám sát ở lớp mạng; giám sát lớp máy chủ; giám sát lớp ứng dụng; giám sát lớp thiết bị đầu cuối.

Ngoài các nội dung liên quan đến giải pháp giám sát, cơ quan tổ chức cần xác định dung lượng lưu trữ cần thiết để lưu trữ nhật ký hệ thống căn cứ vào phạm vi và quy mô giám sát và tổng số tương đối sự kiện của hệ thống phải xử lý trong 01 giây.

Dưới đây là nội dung hướng dẫn cụ thể cho việc thiết lập và quản lý vận hành hệ thống giám sát.

2. Đối tượng, phạm vi giám sát

2.1. Xác định phạm vi giám sát

Về cơ bản, phạm vi giám sát có thể là một hệ thống thông tin, nhiều hệ thống thông tin, một vùng mạng hoặc một đối tượng giám sát cụ thể.

Phạm vi giám sát được xác định dựa vào thẩm quyền, phạm vi quản lý các đối tượng giám sát của cơ quan, tổ chức.

Trường hợp phạm vi giám sát là một hệ thống thông tin là trường hợp hệ thống được triển khai tập trung tại một khu vực địa lý bao gồm các kết nối mạng nội bộ và mạng Internet mà không có kết nối mạng diện rộng đi các mạng khác thuộc phạm vi quản lý của cơ quan, tổ chức.

Trường hợp phạm vi giám sát là nhiều hệ thống thông tin là trường hợp một hệ thống thông tin tổng thể thuộc phạm vi quản lý của cơ quan, tổ chức nhưng có các hệ thống thành phần khác nhau ở khu vực địa lý khác nhau và có kết nối mạng diện rộng về hệ thống trung tâm.

Trường hợp phạm vi giám sát là một vùng mạng như vùng DMZ, vùng cơ sở dữ liệu, vùng quản trị…thì các máy chủ, ứng dụng trong đó sẽ được coi là đối tượng thành phần trong đối tượng giám sát là vùng mạng.

Trường hợp phạm vi giám sát là một đối tượng giám sát cụ thể. *Ví dụ trường hợp thuê dịch vụ giám sát cho máy chủ hay một ứng dụng cụ thể.*

2.2. Xác định đối tượng giám sát

Đối tượng giám sát về cơ bản bao gồm máy chủ, thiết bị mạng, thiết bị bảo

mật, máy chủ, dịch vụ, ứng dụng, các thiết bị đầu cuối và điểm giám sát trên đường truyền, cụ thể:

Hình 1. Đối tượng và lớp giám sát

a) Các thiết bị mạng, thiết bị bảo mật như: Router, Switch, Firewall/IPS/IDS, Sandbox, WAF, Network APT...;

b) Các máy chủ hệ thống (cả máy chủ vật lý và ảo hóa) trên các nền tảng khác nhau: Windows, Linux, Unix…;

c) Các ứng dụng: (1) Ứng dụng phục vụ hoạt động của hệ thống: DHCP, DNS, NTP, VPN, Proxy Server…; (2) Ứng dụng cung cấp dịch vụ: Web, Mail, FPT, TFTP và các hệ quản trị cơ sở dữ liệu Oracle, SQL, MySQL ...;

d) Các thiết bị đầu cuối: Máy tính người sử dụng, máy in, máy fax, IP Phone, IP Camera…;

đ) Điểm giám sát trên đường truyền: Điểm giám sát biên tại giao diện kết nối của thiết bị định tuyến biên với các mạng bên ngoài; điểm giám sát tại mỗi vùng mạng của hệ thống.

2.3. Triển khai giám sát ở lớp mạng

Việc triển khai giám sát ở lớp mạng cho phép phát hiện:

- Các kết nối, truy vấn tới các máy chủ điều khiển mạng botnet (C&C Server);

- Các file mã độc, URL nguy hiểm được truyền qua môi trường mạng (với

các giao thức không mã hóa) bằng cách giải mã giao thức, bóc tách dữ liệu dạng file, URL đưa vào các hệ thống phân tích tự động;

- Các Shellcode, payload tấn công khai thác lỗ hổng phần mềm, dịch vụ trong dữ liệu truyền tải trên mạng thông qua phân tích các dấu hiệu đặc trưng;

- Các hành vi bất thường như dò quét mạng, dò quét tài khoản mật khẩu mặc định, mật khẩu yếu…

Phương án triển khai giám sát trên môi trường mạng phù hợp với việc giám sát lưu lượng mạng không sử dụng các giao thức mã hóa (SSH, VPN, TLS, SSL…). Trường hợp, phương án kỹ thuật yêu cầu cần giám sát lưu lượng mạng có mã hóa thì các thiết bị bảo mật phải có chức năng giải mã hoặc sử dụng thiết bị giải mã chuyên dụng.

Để triển khai giám sát trên môi trường mạng, phương án kỹ thuật yêu cầu phải thiết lập các điểm giám sát như đã được mô tả trong mục 2.2.

Tại mỗi điểm giám sát có thể triển khai hai hình thức Inline và Passive. Mỗi hình thức triển khai có ưu, nhược điểm khác nhau.

Với hình thức Inline, lưu lượng giám sát sẽ đi qua thiết bị giám sát, bảo vệ như Firewall, IDS/IPS…Ưu điểm của hình thức triển khai này là có thể vừa phát hiện và thực hiện ngăn chặn tấn công mạng trực tiếp. Tuy nhiên, điểm hạn chế của hình thức triển khai này là ảnh hưởng đến hiệu năng, thông lượng của lưu lượng mạng do mọi gói tin phải được kiểm tra hợp lệ mới được cho phép đi qua thiết bị bảo vệ. Trường hợp hiệu năng của thiết bị bảo vệ không đủ so với lưu lượng thực tế của hệ thống sẽ làm tắc nghẽn hoặc gây gián đoạn hoạt động của hệ thống nếu thiết bị bảo vệ xảy ra sự cố. Trường hợp triển khai theo phương án này thì giải pháp bảo vệ cần bảo đảm đủ hiệu năng, có phương án cân bằng tải, dự phòng nóng và có chức năng bypass traffic khi thiết bị quá tải hoặc có sự cố.

Với hình thức Passive, lưu lượng mạng sẽ được trích rút ra để phân tích bằng cách sử dụng thiết bị trích rút dữ liệu (Network-TAP) hoặc sử dụng chức năng span port trên các Switch. Ưu điểm hình thức triển khai này là không làm ảnh hưởng đến hiệu năng, thông lượng lưu lượng mạng. Tuy nhiên, hình thức này không ngăn chặn trực tiếp được các tấn công mạng mà chỉ đưa ra cảnh báo. Để giải quyết vấn đề này, giải pháp sử dụng cần có chức năng tương tác với các thiết bị mạng, thiết bị bảo mật hay máy chủ để ngăn chặn tấn công.

Việc sử dụng Network-TAP hay span port cần chú ý là dữ liệu trích rút cần có hai chiều (từ ngoài vào hệ thống và bên trong hệ thống đi ra). Một số thiết bị Network-TAP chỉ trích rút dữ liệu theo từng chiều và đưa ra cổng ra tương ứng. Do đó trường hợp thiết bị bảo vệ chỉ có 01 cổng phân tích thì sẽ chỉ phân tích được một lưu lượng mạng một chiều. Do đó, Network-TAP cần được lựa chọn loại có chức năng Aggregator để cho phép trích rút hai chiều lưu lượng mạng và đưa vào 01 cổng ra.

2.4. Triển khai giám sát lớp máy chủ

Việc triển khai giám sát ở lớp máy chủ cho phép phát hiện:

- Các hành vi vi phạm chính sách truy cập, quản lý, thiết lập cấu hình hệ điều hành, các dịch vụ hệ thống;

- Các kết nối của máy chủ ra các địa chỉ IP độc hại;

- Các hình thức tấn công mạng như tấn công khai thác điểm yếu, tấn công dò quét và các dạng tấn công tương tự khác;

- Sự thay đổi trái phép của các tệp tin hệ thống;

- Các tiền trình có dấu hiệu bất thường về hành vi và việc sử dụng tài nguyên máy chủ;

Việc triển khai giám sát ở lớp máy chủ cho phép giải quyết được vấn đề của triển khai giám sát lớp mạng là thường không phụ thuộc vào các lưu lượng mạng có mã hóa. Tuy nhiên, việc triển khai giám sát lớp máy chủ sẽ ảnh hưởng đến tài nguyên của máy chủ và khả năng mở rộng phạm vi giám sát khi số lượng máy chủ lớn. Do đó, cần lựa chọn các giải pháp cho phép quản lý tập trung để giảm thiểu việc xử lý trực tiếp các chức năng giám sát trên từng máy chủ.

Việc triển khai giám sát lớp máy chủ có thể triển khai theo hai hình thức sau:

- Cài đặt phần mềm giám sát có chức năng phát hiện tấn công trực tiếp trên máy chủ như Host IDS, AV, DLP…Hình thức này chức năng phát hiện tấn công hay các hành vi vi phạm được phát hiện trực tiếp và gửi nhật ký cảnh báo về hệ thống quản lý tập trung;

- Gửi log về hệ thống giám sát tập trung như SIEM. Hình thức này chức năng phát hiện tấn công mạng được thực hiện trên hệ thống quản lý tập trung thông qua việc phân tích dấu hiệu, luật tương quan hay sử dụng công nghệ dữ liệu lớn. Việc gửi log về hệ thống giám sát tập trung có thể thực hiện thông qua các giao thức hệ điều hành hỗ trợ như Syslog, SNMP hoặc các Agent của những giải pháp cụ thể.

Hình thức gửi log về hệ thống giám sát tập trung sẽ ít ảnh hưởng đến hiệu năng của máy chủ so với hình thức trên. Tuy nhiên, hình thức này sẽ không thể phát hiện được một số dạng tấn công mà giải pháp sử dụng cần phân tích nhiều thông tin tương quan khác trên máy chủ.

Trường hợp gửi log về hệ thống giám sát tập trung thì cần lựa chọn nguồn log có thông tin để phục vụ các giải pháp phát hiện tấn công. Nguồn log gửi về cần tối thiểu có các thông tin sau:

- Thông tin kết nối mạng tới máy chủ (Firewall log);

- Thông tin đăng nhập vào máy chủ;

- Lỗi phát sinh trong quá trình hoạt động (nhật ký trạng thái hoạt động của máy chủ);

- Thông tin về các tiến trình hệ thống;

- Thông tin về sự thay đổi các tập tin, thư mục trên hệ thống;

- Thông tin thay đổi cấu hình máy chủ.

2.5. Triển khai giám sát lớp ứng dụng

Việc triển khai giám sát lớp ứng dụng cho phép phát hiện:

- Các dạng tấn công vào lớp ứng dụng như SQLi, XSS...;

- Tấn công dò quét, vét cạn mật khẩu, thư mục và khai thác thông tin;

- Tấn công thay đổi giao diện;

- Tấn công Phishing và cài cắm mã độc trên ứng dụng;

- Tấn công từ chối dịch vụ.

Việc triển khai giám sát ở mức mạng cũng có thể phát hiện các dạng tấn công ở trên trong trường hợp lưu lượng mạng không có mã hóa.

Hình thức triển khai giám sát lớp ứng dụng cũng được thực hiện tương tự đối với lớp hệ điều hành. Chỉ khác là lựa chọn phần mềm và giải pháp phù hợp cho phát hiện tấn công lớp ứng dụng. *Ví dụ để phát hiện tấn công ứng dụng web có thể sử dụng phần mềm tường lửa ứng dụng web hoặc phần mềm Host IDS được cài đặt trực tiếp trên máy chủ.*

Trường hợp gửi log về hệ thống giám sát tập trung thì cần lựa chọn nguồn log có thông tin để phục vụ các giải pháp phát hiện tấn công. Nguồn log gửi về cần tối thiểu có các thông tin sau:

- Thông tin truy cập ứng dụng;

- Thông tin đăng nhập khi quản trị ứng dụng;

- Thông tin các lỗi phát sinh trong quá trình hoạt động;

- Thông tin thay đổi cấu hình ứng dụng.

2.6. Triển khai giám sát lớp thiết bị đầu cuối

Các thiết bị đầu cuối ngoài máy tính người sử dụng thì các thiết bị khác không hỗ trợ cài đặt các phần mềm bảo vệ trên thiết bị. Việc giám sát bảo vệ máy tính của người sử dụng có thể thực hiện tương tự như đối với máy chủ.

Các thiết bị đầu cuối khác không hỗ trợ cài đặt phần mềm bảo vệ thì có thể triển khai giám sát theo hai hình thức sau: Bật chức năng gửi Syslog trên thiết bị hoặc kết nối, lấy dữ liệu về để phân tích sử dụng giao thức SNMP (hoặc giao

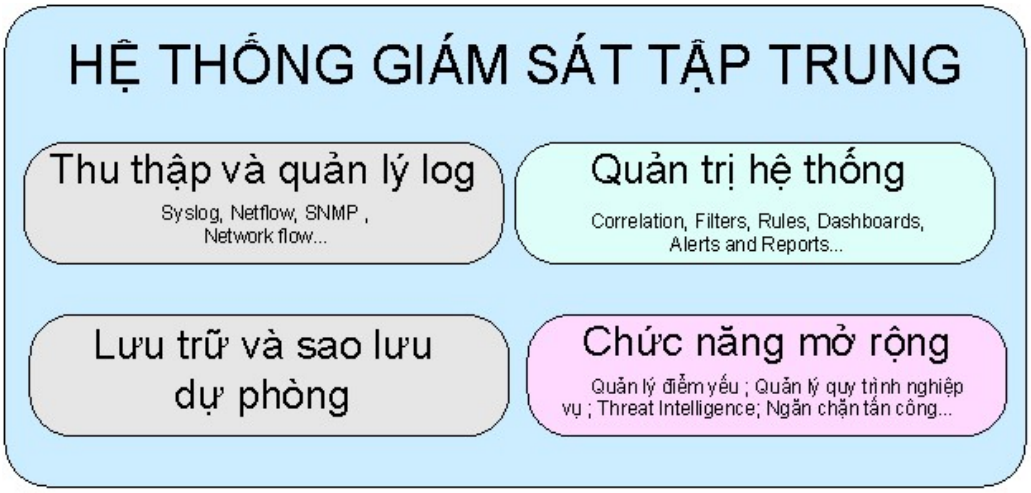
thức có chức năng tương đương).

Việc giám sát thiết bị đầu cuối nên kết hợp với giám sát thiết bị quản lý truy cập NAC để phát hiện các thiết bị đầu cuối vi phạm chính sách của hệ thống. Ngoài ra cần đồng bộ với việc cấp phát địa chỉ IP của máy chủ DHCP để có thể xác định các thiết bị đầu cuối vi phạm chính sách dựa vào địa chỉ MAC.

3. Hệ thống quản lý tập trung

3.1. Yêu cầu cơ bản đối với hệ thống quản lý tập trung

Yêu cầu đối với hệ thống quản lý tập trung cần đáp ứng các yêu cầu theo quy định tại Điều 5, khoản 1 Thông tư số 31/2017/TT-BTTTT và các yêu cầu cụ thể dưới đây:



Hình 2. Yêu cầu chức năng đối với hệ thống quản lý tập trung

a) Chức năng quản trị

- Chức năng phân tích tương quan (Correlation): Chức năng này cho phép phân tích tương quan thông tin giữa các log nhận được từ các đối tượng giám sát khác nhau;

- Chức năng lọc (Filters): Cho phép lọc ra log cần truy vấn dựa theo nội dung của từng trường thông tin mà nguồn log đã được chuẩn hóa và lưu trữ;

- Tạo các luật (Rules): Cho phép người quản trị thiết lập các luật kết hợp giữa chức năng Filter và các luật tương quan để phát hiện ra tấn công mạng hay hành vi bất thường của người sử dụng;

- Chức năng hiển thị (Dashboards): Cung cấp giao diện quản trị hệ thống, thông tin thống kê và quản lý sự kiện nhận được theo thời gian thực;

- Chức năng cảnh báo và báo cáo (Alerts and Reports): Cho phép quản lý thông tin cảnh báo và tạo báo cáo;

- Chức năng cảnh báo thời gian thực (Real Time Alert) cho phép gửi thông

tin cảnh báo thời gian thực từ hệ thống ngay khi có sự cố xảy ra.

b) Chức năng nhận log

- Cho phép nhận log từ các nguồn với nhiều định dạng khác nhau từ các thiết bị mạng, máy chủ và ứng dụng;

- Cung cấp các chức năng cho phép định dạng, chuẩn hóa log nhận được theo các trường thông tin tùy biến theo nhu cầu sử dụng;

- Cho phép nhận log trực tiếp qua các giao thức mạng như: Syslog, Netflow, SNMP và các giao thức có chức năng tương đương theo thiết kế của từng hãng cụ thể. Giao thức truyền, nhận log qua môi trường mạng cần hỗ trợ chức năng mã hóa dữ liệu, nén dữ liệu;

- Cho phép tải các tệp tin log theo các định dạng khác nhau lên hệ thống để chuẩn hóa và phân tích.

c) Yêu cầu về lưu trữ

Yêu cầu lưu trữ đối với hệ thống quản lý tập trung cần bảo đảm thời gian tối thiểu để lưu trữ nhật ký hệ thống căn cứ vào cấp độ (Điều 9 Thông tư số 03/2017/TT-BTTTT) của hệ thống thông tin được triển khai giám sát, cụ thể:

- Hệ thống thông tin cấp độ 1 hoặc 2 là 01 tháng.

- Hệ thống thông tin cấp độ 3 là 03 tháng.

- Hệ thống thông tin cấp độ 4 là 06 tháng.

- Hệ thống cấp độ 5 là 12 tháng.

d) Chức năng mở rộng

- Quản lý điểm yếu an toàn thông tin;

- Quản lý quy trình nghiệp vụ xử lý sự cố an toàn thông tin;

- Tích hợp, tổng hợp và phân tích thông tin từ hệ thống Threat Intelligence;

- Tự động tương tác với thiết bị mạng và máy chủ để ngăn chặn tấn công.

3.2. Nguyên lý hoạt động cơ bản

Hệ thống quản lý tập trung cho phép nhận quản lý tập trung log từ nhiều nguồn và định dạng của các thiết bị, máy chủ và ứng dụng khác nhau. Việc quản lý log trên một hệ thống tập trung ngoài việc cho phép quản lý tổng thể các sự kiện xảy ra trong hệ thống còn cho phép phân tích, truy vết và phát hiện tấn công mạng. Về cơ bản, hoạt động của hệ thống như sau:

a) Đối tượng giám sát gửi log về hệ thống giám sát tập trung bằng một trong các hình thức sau:

- Đối với đối tượng giám sát là các thiết bị mạng, thiết bị bảo mật phải thiết lập chức năng gửi log về hệ thống tập trung sử dụng một số giao thức mà thiết bị đó hỗ trợ. Giao thức phổ biến mà thiết bị hỗ trợ là Syslog, SNMP và Netflow.

- Đối tượng giám sát là các máy chủ hoặc các thiết bị khác cho phép cài đặt Agent (do hãng cung cấp giải pháp phát triển) để gửi log về hệ thống tập trung. Hình thức này cho phép tùy biến cao các nguồn log có thể gửi về hệ thống tập trung như log của hệ điều hành, ứng dụng, tường lửa mềm…Các Agent cung cấp chức năng nén, mã hóa dữ liệu trước khi gửi log về hệ thống tập trung.

Trường hợp khi số lượng đối tượng giám sát lớn và nằm phân tán ở nhiều hệ thống mạng khác nhau thì các đối tượng giám sát xem xét được chia thành từng nhóm theo từng hệ thống mạng và được thiết lập gửi log về một điểm trung gian. Điểm nhận log trung gian này cho phép nhận log từ các điểm giám sát nén và mã hóa dữ liệu trước khi gửi về hệ thống tập trung.

b) Dữ liệu nhận được từ hệ thống tập trung sẽ được chuẩn hóa theo từng định dạng mà hệ thống đó hỗ trợ. Trường hợp định dạng log mới mà hệ thống chưa hỗ trợ thì sẽ có chức năng cho phép người sử dụng tự định nghĩa định dạng log để chuẩn hóa. Ngoài chức năng chuẩn hóa dữ liệu, hệ thống quản lý tập trung còn cung cấp chức năng cho phép lọc bỏ các log trùng lặp hoặc không cần thiết trước khi lưu vào cơ sở dữ liệu.

Dữ liệu log sau khi được chuẩn hóa và lưu vào cơ sở dữ liệu cho phép người sử dụng quản lý, phân tích để truy vết và phát hiện tấn công mạng.

Hệ thống quản lý tập trung thường tích hợp các chức năng tự động phát hiện tấn công trên cơ sở phân tích log nhận được. Chức năng phát hiện tấn công có thể được thiết lập dựa vào các luật phân tích tương quan, các dấu hiệu tấn công; sử dụng hệ thống Threat Intelligence hoặc áp dụng công nghệ: AI, Data mining, Big Data…

Tấn công mạng sau khi được phát hiện, hệ thống quản lý tập trung sẽ thực hiện các hành động cụ thể theo chính sách của người sử dụng đưa vào như: gửi cảnh báo qua email, SMS hoặc tương tác với các thiết bị mạng, thiết bị bảo mật để tự động ngăn chặn tấn công. Các hành động cụ thể được hiển thị dưới dạng các cảnh báo theo thời gian thực cho phép người quản trị giám sát, theo dõi.

4. Thiết lập hệ thống

4.1. Cài đặt hệ thống

Việc cài đặt thành phần xử lý tập trung phụ thuộc vào gói giải pháp được đầu tư. Đối với các giải pháp được đầu tư tích hợp cùng phần cứng của hãng dưới dạng thiết bị chuyên dụng thì không yêu cầu quá trình cài đặt mà chỉ cần thiết lập cấu hình để sử dụng.

Đối với gói giải pháp dưới dạng phần mềm được cài đặt trên hệ điều hành thì trước hết cần lựa chọn hệ điều hành phù hợp và tiến hành cài đặt. Căn cứ vào

yêu cầu về năng lực xử lý của phần mềm giám sát đối với máy chủ để lựa chọn máy chủ và không gian lưu trữ phù hợp. Khuyến khích cơ quan, tổ chức triển khai cài đặt giải pháp trên nền tảng ảo hóa để dễ dạng mở rộng, nâng cấp và sao lưu dự phòng.

Chú ý việc cài đặt hệ thống cần thực hiện trên môi trường độc lập với hệ thống đang hoạt động của cơ quan, tổ chức để tránh các ảnh hưởng không cần thiết đến hệ thống đang hoạt động.

Sau khi cài đặt thiết lập hệ thống thì cần nâng cấp phiên bản, cập nhật các bản vá và thực hiện kiểm tra đánh giá an toàn thông tin cho hệ thống trước khi đưa vào sử dụng. Thông tin về các điểm yếu an toàn thông tin có thể được tham khảo tại địa chỉ: https://ti.khonggianmang.vn/, https://www.cvedetails.com/...

4.2. Thiết lập cấu hình hệ thống

Để đưa hệ thống giám sát vào hệ thống, thì người quản trị cần quy hoạch địa chỉ IP, vùng mạng và các chính sách truy cập trên các thiết bị bảo vệ trước khi kết nối hệ thống giám sát vào hệ thống.

Hệ thống giám sát cần được đưa vào một vùng mạng riêng (vùng quản trị thiết bị hệ thống). Vùng mạng này sẽ được quy hoạch địa chỉ IP cho giao diện quản trị trên các thiết bị/máy chủ và giao diện của hệ thống giám sát cho phép việc gửi/nhận log được gửi trực tiếp giữa các giao diện trong vùng mạng này mà không qua các thiết bị mạng trung gian để không ảnh hưởng đến các kết nối mạng khác trong hệ thống.

Hệ thống giám sát cần được bảo vệ với các thiết bị bảo mật và được thiết lập cấp hình bảo mật tối thiểu bao gồm: Kiểm soát truy cập từ các vùng mạng khác đi vào vùng quản trị thiết bị hệ thống; Kiểm soát truy cập từ vùng quản trị thiết bị hệ thống đi ra các vùng mạng khác; Phòng chống xâm nhập; Phòng chống phần mềm độc hại trên môi trường mạng.

Vùng mạng quản trị cần được thiết lập riêng để đặt các máy tính quản trị, vận hành hệ thống giám sát. Các thiết bị bảo mật cần được thiết lập chỉ cho phép các máy tính quản trị được truy cập, quản lý hệ thống giám sát.

Trường hợp cần quản trị hệ thống giám sát từ xa thì cần thiết lập cấu hình hệ thống để cho phép truy cập gián tiếp từ các máy bên ngoài vào các máy quản trị thông qua các giao thức mạng có mã hóa, bảo mật như VPN, SSH, TLS, SSL …

4.3. Kiểm thử nghiệm thu hệ thống giám sát

Hệ thống giám sát cần được cài đặt trên môi trường độc lập, sau khi cài đặt và kiểm thử hệ thống thì mới đưa vào khai thác, vận hành trong môi trường thực tế.

Căn cứ vào các yêu cầu đối với hệ thống giám sát, cơ quan, tổ chức yêu cầu

đơn vị cung cấp giải pháp xây dựng kịch bản kiểm thử để đánh giá khả năng đáp ứng của hệ thống. Trong đó, kịch bản kiểm thử cần đáp ứng tối thiểu các nội dung sau:

- Các hình thức tiếp nhận log từ các thiết bị giám sát, trực tiếp qua các giao thức mạng hoặc gián tiếp qua việc tải tệp tin log lên hệ thống;

- Khả năng nhận và chuẩn hóa định dạng log của các thiết bị, máy chủ, ứng dụng và dịch vụ khác nhau (đối với định dạng hệ thống đã hỗ trợ) và khả năng tùy biến để chuẩn hóa định dạng log mới (đối với định dạng hệ thống chưa hỗ trợ);

- Số lượng sự kiện tối đa mà hệ thống có thể tiếp nhận và xử lý trong một giây;

- Các chức năng của hệ thống để đáp ứng các yêu cầu về mặt chức năng như được mô tả tại mục 3.1 như: Lọc, phân tích tương quan, thiết lập luật trên thành phần quản lý tập trung; phân tích thống kê; cảnh báo và báo cáo.

5. Quản lý, vận hành hệ thống

Để đưa hệ thống giám sát vào vận hành, khai thác hiệu quả thì cơ quan, tổ chức cần xây dựng quy định, quy trình quản lý vận hành hệ thống giám sát. Các quy định này có thể được đưa vào Quy chế bảo đảm an toàn thông tin của tổ chức để triển khai thực hiện.

Cơ quan, tổ chức có thể tham khảo tiêu chuẩn quốc gia TCVN 11930:2017, để xây dựng các quy định và quy trình liên quan đến quản lý, vận hành hệ thống giám sát bao gồm:

5.1. Quản lý, vận hành hoạt động bình thường của hệ thống

Các quy định, quy trình liên quan đến quản lý, vận hành hoạt động bình thường của hệ thống giám sát là các quy định, quy trình nhằm bảo đảm hệ thống giám sát hoạt động ổn định, có tính chịu lỗi cao và sẵn sàng khôi phục lại trạng thái bình thường khi xảy ra sự cố. Các quy định, quy trình cần tối thiểu bao gồm các nội dung:

- Khởi động và tắt hệ thống giám sát;

- Thay đổi cấu hình và các thành phần của hệ thống giám sát;

- Quy trình xử lý các sự cố liên quan đến hoạt động của hệ thống giám sát;

- Quy trình sao lưu, dự phòng cấu hình hệ thống và log của hệ thống;

- Quy trình bảo trì, nâng cấp hệ thống giám sát;

- Quy trình khôi phục hệ thống sau sự cố.

5.2. Kết nối và gửi log từ đối tượng giám sát về hệ thống quản lý tập trung

Đối tượng giám sát của hệ thống có nhiều loại khác nhau, mỗi loại có định dạng log và chức năng hỗ trợ gửi log cũng khác nhau. Thêm nữa, đối tượng giám sát có thể nằm phân tán ở nhiều vị trí khác nhau. Do đó, cần có quy định và quy trình gửi log từ đối tượng giám sát về hệ thống quản lý tập trung. Quy định, quy trình liên quan đến nội dung này có thể bao gồm:

- Loại log mà hệ thống có thể tiếp nhận;

- Giao thức gửi nhận log hệ thống hỗ trợ;

- Quy định về quy tắc xác định nguồn gửi log như đặt tên thiết bị theo quy tắc;

- Số lượng sự kiện tối đa từ một đối tượng giám sát có thể gửi;

- Chính sách hệ thống để quản lý các nguồn log gửi về;

- Quy định về chuẩn mã hóa, nén dữ liệu.

5.3. Truy cập và quản trị hệ thống

Hệ thống giám sát lưu trữ nhiều thông tin quan trọng của hệ thống. Do đó, việc truy cập và quản trị hệ thống giám sát cần được quy định và có các quy trình để thực hiện. Các quy định, quy trình liên quan đến nội dung này có thể bao gồm:

- Chính sách truy cập, quản trị hệ thống từ mạng bên trong hệ thống và từ xa;

- Quản lý tài khoản và phân quyền truy cập, quản trị hệ thống;

- Truy cập và quản lý tập tin cấu hình và log lưu trữ trên hệ thống;

- Quyền thiết lập cấu hình và quản lý các đối tượng giám sát.

5.4. Lưu trữ và bảo vệ log hệ thống

Log hệ thống là dữ liệu quan trọng của cơ quan, tổ chức cần bảo vệ. Việc lộ lọt dữ liệu log hệ thống có thể là cơ sở để tin tặc khai thác thông tin của hệ thống phục vụ việc thực hiện các cuộc tấn công mạng. Do đó, việc lưu trữ và bảo vệ log hệ thống cần được quy định và có quy trình để thực hiện. Các quy định, quy trình liên quan đến nội dung này có thể bao gồm:

- Loại log và thông tin cấu hình hệ thống cần lưu trữ;

- Tần suất sao lưu, dự phòng tập tin cấu hình và log hệ thống;

- Gán nhãn dữ liệu (quy cách đặt tên, nơi lưu trữ…), mã hóa, nén dữ liệu log;

- Khôi phục và bảo vệ log hệ thống khi xảy ra sự cố theo phương án và năng lực xử lý của cơ quan, tổ chức.

5.5. Theo dõi, giám sát, cảnh báo và xử lý tấn công mạng

Một trong những nội dung quan trọng liên quan đến quản lý, vận hành hệ thống giám sát là quy định, quy trình theo dõi, giám sát, cảnh báo và xử lý tấn công mạng. Các hình thức tấn công mạng tùy thuộc vào mức độ nghiêm trọng sẽ có các phương án xử lý khác nhau. Để chủ động đối phó với các dạng tấn công mạng được ghi nhận trên hệ thống, cơ quan tổ chức cần quy định và có quy trình xử lý. Các quy định, quy trình liên quan đến nội dung này có thể bao gồm:

- Quy định trách nhiệm của cán bộ trong việc thực hiện theo dõi, giám sát, cảnh báo và xử lý tấn công mạng;

- Quy trình thực hiện theo dõi, giám sát, cảnh báo và xử lý tấn công mạng;

- Quy trình thu thập thông tin và quản lý, cập nhật xử lý các sự cố mới;

- Quy định về các mức độ sự cố tấn công mạng và xây dựng quy trình xử lý tấn công mạng đối với các dạng tấn công cụ thể, tối thiểu bao gồm:

+ Tấn công dò, quét và khai thác thông tin hệ thống;

+ Tấn công mã độc, tấn công có chủ đích;

+ Tấn công khai thác điểm yếu, chiếm quyền điều khiển hệ thống;

+ Tấn công thay đổi giao diện;

+ Tấn công đánh cắp dữ liệu hoặc phá hoại dữ liệu;

+ Tấn công từ chối dịch vụ.

- Quy định về việc định kỳ tổ chức thực hành, diễn tập xử lý sự cố tấn công mạng.

- Quy định về chế độ báo cáo khi phát hiện và xử lý sự cố tấn công mạng.

5.6. Bố trí nguồn lực và tổ chức giám sát

Cơ quan, tổ chức cần bố trí cán bộ và tổ chức giám sát 24/7 (đối với hệ thống thông tin cấp độ 3 trở lên). Tùy thuộc vào nguồn nhân lực của mỗi cơ quan, tổ chức mà các cán bộ được bố trí làm cán bộ chuyên trách hay kiêm nhiệm các nhiệm vụ trong việc vận hành hệ thống giám sát hoặc một cán bộ có thể thực hiện nhiệm vụ của nhiều nhóm khác nhau.

Về cơ bản các nhiệm vụ trong quá trình quản lý vận hành hệ thống giám sát được phân làm các nhóm công việc sau:

a) Nhóm quản lý vận hành hệ thống giám sát

- Có nhiệm vụ quản lý vận hành bảo đảm các hoạt động bình thường của hệ

thống giám sát. Nhóm này có thể nằm trong nhóm quản lý vận hành chung cho toàn bộ hạ tầng của hệ thống.

- Có kiến thức về mạng, nắm được thiết kế hệ thống, thiết lập cấu hình bảo mật trên các thiết bị, máy chủ.

- Phải theo dõi, thường xuyên, liên tục trạng thái hoạt động của hệ thống, tài nguyên, băng thông, trạng thái kết nối để bảo đảm hệ thống hoạt động bình thường, có tính sẵn sàng cao.

b) Nhóm theo dõi và cảnh báo

- Có nhiệm vụ theo dõi, giám sát các sự kiện, tấn công mạng ghi nhận được trên hệ thống. Xác định và phân loại mức độ sự cố và xác định hành động phù hợp tiếp theo hoặc cảnh báo cho nhóm xử lý sự cố thực hiện.

- Có kiến thức về các lỗ hổng mới, mã độc mới, chiến dịch, hình thức tấn công mới; có thể phân loại và xác định mức độ của các sự cố và tìm kiếm, truy vấn thông tin từ các nguồn dữ liệu bên ngoài như hệ thống Threat Intelligence.

- Thực hiện định kỳ phân tích bộ luật, cảnh báo sai thực hiện whitelist, chỉnh sửa luật không cho những cảnh báo sai lập lại để tối ưu khả năng phát hiện tấn công, sự cố của hệ thống, giảm thiểu nhận diện nhầm.

c) Nhóm xử lý sự cố

- Có nhiệm vụ tiếp nhận cảnh báo, xác minh và thực hiện các hành động để xử lý sự cố, bao gồm một số hành động cụ thể như sau:

- Xác định các hành động ứng cứu khẩn cấp: Phản ứng chặn kênh kết nối điều khiển, bổ sung luật ngăn chặn sớm tấn công hoặc cô lập hệ thống.

- Xử lý các lỗ hổng, điểm yếu, cập nhật bản vá và bóc gỡ mã độc trên hệ thống;

Nâng cấp hoặc khôi phục hệ thống sau sự cố.

d) Nhóm điều tra, phân tích

- Có nhiệm vụ phân tích chuyên sâu các cảnh báo, các sự cố để tìm ra nguồn gốc, nguyên nhân và các dấu hiệu nhận biết tấn công.

- Kết quả đầu ra của nhóm này là chứng cứ số, các dấu hiệu cho phép thiết lập các tập luật trên hệ thống để ngăn chặn các dạng tấn công tương tự tiếp theo đến hệ thống./.